

PRICE AND GESS

ATTORNEYS AT LAW

JOSEPH W. PRICE
ALBIN H. GESS
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE

OF COUNSEL
JAMES F. KIRK

2100 S.E. MAIN STREET, SUITE 250
IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pgu@pgulaw.com



PRIORITY DOCUMENT

(Japan 2001-002177)

Inventor(s): Hiroki Taoka et al.

Title: CONTENT DECRYPTION DEVICE

Attorney's

Docket No.: NAK1-BQ89

EXPRESS MAIL LABEL NO. EL 873068990 US

DATE OF DEPOSIT: January 9, 2002

JOSEPH W. PRICE 949-261-8433

HIROKI TAOKA

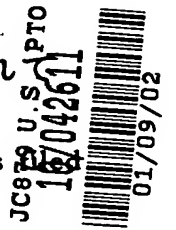
日本国特許庁

JAPAN PATENT OFFICE

NAK1-BQ89

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as with this Office



出願年月日

Date of Application:

2001年 1月10日

出願番号

Application Number:

特願2001-002177

出願人

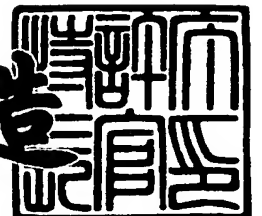
Applicant(s):

松下電器産業株式会社

2001年10月 1日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3089718

【書類名】 特許願

【整理番号】 2022520379

【提出日】 平成13年 1月10日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/28

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 田岡 宏毅

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 湯川 泰平

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 セキュアなコンテンツ転送装置

【特許請求の範囲】

【請求項 1】 暗号化されたコンテンツを蓄積するデータ記録部と、暗号化されたコンテンツを復号する機能を有する中央演算装置と、復号されたコンテンツを出力するコンテンツ出力部を有する復号装置であって、

前記中央演算装置は、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

前記データ記録部から読み出した暗号データの復号処理を行う復号処理部と、

前記復号処理部で復号されたデータを格納する復号データ格納部と、

前記コンテンツ出力部のアドレスを含む、前記復号されたデータを転送しても良いアドレスを格納する転送先アドレス格納部と、

前記命令実行部が前記復号データ格納部に格納されているデータの転送を指示した時、転送先のアドレスが前記転送先アドレス格納部に格納されているか否かを検査する転送是非判定部とを有し、

前記転送是非判定部は検査結果が否定である場合、命令実行部からの前記復号されたデータの転送指示を指示通りに実行しないことを特徴とする復号装置。

【請求項 2】 前記復号装置は内部にバスを有し、

前記バスには前記中央演算装置と、前記コンテンツ出力部と、前記命令実行部が実行する前記ソフトウェアを格納するメモリーと、外部機器とのデータの入出力を行う外部インターフェース部とが接続され、

前記ソフトウェアは前記外部インターフェース部を介して外部からダウンロードすることが可能であることを特徴とする請求項 1 記載の復号装置。

【請求項 3】 前記中央演算装置は、

転送先アドレスに関する暗号化された情報を復号する転送先アドレス復号部を有し、

前記転送先アドレス格納部の内容は前記転送先アドレス復号部の出力に応じて書き換え可能であることを特徴とする請求項 1 または 2 記載の復号装置。

【請求項 4】 前記中央演算装置は、

前記転送先アドレス格納部の内容が設定済みか未設定であることを判定する転送先アドレス設定判定部を有し、

前記転送先アドレス設定判定部が未設定と判定した場合、命令実行部からの前記復号されたデータの転送指示を指示通りに実行しないことを特徴とする請求項 1 または 2 または 3 に記載の復号装置。

【請求項 5】 前記中央演算装置はさらに、

暗号鍵を格納する暗号鍵格納部を有し、

前記復号処理部は前記暗号鍵格納部に設定された暗号鍵を用いて復号処理を行うことを特徴とする請求項 1 または 2 または 3 または 4 に記載の復号装置。

【請求項 6】 前記中央演算装置はさらに、

暗号化された暗号鍵を復号する暗号鍵復号部を有し、

前記暗号鍵格納部は固定値である第 1 の鍵と、データの復号に用いる可変値の第 2 の鍵を格納することができ、前記暗号鍵復号部は前記第 1 の鍵で暗号化された第 2 の鍵の入力を受け、これを前記第 1 の鍵を用いて復号し、復号された第 2 の鍵を前記暗号鍵格納部に格納することにより、第 2 の鍵の変更を行うことができ、

前記復号処理部は前記暗号鍵格納部に設定された第 2 の暗号鍵を用いて復号処理を行うことを特徴とする請求項 5 に記載の復号装置。

【請求項 7】 前記中央演算装置はさらに、

前記暗号格納部の中の前記第 2 の鍵が設定済みか未設定であることを判定する暗号鍵設定判定部を有し、

前記暗号鍵設定判定部が未設定と判定した場合、前記命令実行部からのデータの復号指示を指示通りに実行しないことを特徴とする請求項 6 に記載の復号装置。

【請求項 8】 復号機能を有する中央演算装置であって、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

暗号データの復号処理を行う復号処理部と、

前記復号処理に用いる 2 種類以上の鍵を格納する暗号鍵格納部と、

2 種類以上の暗号鍵で暗号化された同一のデータの復号結果を前記復号処理部

から入力してこれらを比較する比較手段を有し、

復号結果が一致しないと前記比較手段が判定した場合、命令実行部からの復号されたデータの出力指示を指示通りに実行しないことを特徴とする中央演算装置

。 【請求項 9】 復号機能を有する中央演算装置であって、
ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、
暗号データの復号処理を 2 種類以上の暗号関数で実行する復号処理部と、
前記復号処理に用いる鍵を格納する暗号鍵格納部と、

2 種類以上の暗号関数で暗号化された同一のデータの復号結果を前記復号処理部から入力してこれらを比較する比較手段を有し、

復号結果が一致しないと前記比較手段が判定した場合、命令実行部からの復号されたデータの出力指示を指示通りに実行しないことを特徴とする中央演算装置

。 【請求項 1 0】 前記中央演算装置において、
前記比較手段が復号結果が一致しないと判断した場合に前記中央演算装置の初期化を実行することを特徴とする請求項 8 または 9 に記載の中央演算装置。

【請求項 1 1】 請求項 8 または 9 に記載の中央演算装置と前記中央演算装置を動作させるソフトウェアを格納するソフトウェア格納部とを有し、

前記中央演算装置はさらに、

前記ソフトウェア格納部に格納した前記ソフトウェアが更新されたか否かを判定するソフトウェア更新判定部を有し、

前記比較手段が復号結果が一致しないと判断した場合に、前記ソフトウェア格納部に格納した前記ソフトウェアの更新を要求し、その後前記ソフトウェア更新判定部がソフトウェアは未更新と判定した場合には、前記命令実行部からのデータの復号指示を指示通りに実行しないことを特徴とする復号装置。

【請求項 1 2】 データの書き換えが可能なデータ記録部と、暗号・復号機能を有する中央演算装置とコンテンツ出力部を有する復号装置であって、

前記データ記録部は、

前記中央演算装置と前記コンテンツ出力部の間の共通鍵を暗号化した状態で記

録する暗号化共通鍵記録部を有し、

前記中央演算装置は、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

暗号化された暗号鍵を復号する暗号鍵復号部と、

復号された前記共通鍵や固定値である暗号鍵を格納する暗号鍵格納部とを有し

前記コンテンツ出力部は、前記中央演算装置と同様に、

暗号化された暗号鍵を復号する暗号鍵復号部と、

復号された前記共通鍵や固定値である暗号鍵を格納する暗号鍵格納部とを有し

前記共通鍵が前記中央演算装置と前記コンテンツ出力部の固定の鍵によって別々に暗号化された状態で前記データ記録部内の前記暗号化共通鍵記録部にあらかじめ格納されていて、前記中央演算装置・前記コンテンツ出力部それぞれの前記暗号鍵復号部に転送・復号され、前記暗号鍵格納部に格納されることで共通鍵として設定され、前記データ記録部内の前記暗号化共通鍵記録部の内容の更新によって前記中央演算装置と前記コンテンツ出力部の間の共通鍵を更新することが可能なことを特徴とする装置。

【請求項 1 3】 さらに前記中央演算装置は、

新たな共通鍵を格納する新共通鍵格納部と、

暗号鍵を暗号する処理を実行できる暗号鍵暗号部を有し、

前記中央演算装置は、前記新共通鍵格納部に格納している新しい共通鍵の値を前記暗号鍵暗号部において、現在の共通鍵で暗号化して、前記コンテンツ出力部に転送し、その後前記暗号鍵格納部内の前記共通鍵を前記新たな共通鍵に更新し

前記コンテンツ出力部は、転送された暗号化された前記新たな暗号鍵を前記暗号鍵復号部で復号して、前記暗号鍵格納部に格納し前記共通鍵の値を更新することで、

前記中央演算装置と前記コンテンツ出力部の間の共通鍵が更新可能なことを特徴とする請求項 1 2 記載の装置。

【請求項14】 さらに、前記中央演算装置は、
新たな共通鍵を生成する演算を行う新共通鍵演算部と、
新しい共通鍵の生成に用いるデータXを格納する新共通鍵作成データ格納部と
を有し、
前記コンテンツ出力部は、
前記中央演算装置内の前記新共通鍵演算部と同一の演算を実行する新共通鍵演算部と、
新しい共通鍵の生成に用いるデータXを格納する新共通鍵作成データ格納部と
を有し、
前記中央演算装置は、前記新共通鍵作成データ格納部に格納している前記データXを前記暗号鍵暗号部において、現在の共通鍵で暗号化して、前記コンテンツ出力部に転送し、
前記コンテンツ出力部は、転送された暗号化された前記データXを前記暗号鍵復号部で復号して前記新共通鍵作成データ格納部に格納し、
それぞれ前記中央演算装置、前記コンテンツ出力部の双方で、現在の共通鍵と前記データXから前記新共通鍵演算部を用いて前記新たな共通鍵を算出して、その結果を前記暗号鍵格納部内に格納し共通鍵の値を更新することで、
前記中央演算装置と前記コンテンツ出力部の間の共通鍵が更新可能なことを特徴とする請求項12記載の装置。

【請求項15】 コンテンツを蓄積する外部記録媒体と、前記コンテンツを出力するコンテンツ出力部と、前記外部記録媒体や前記コンテンツ出力部と認証を行う中央演算装置を有する装置であって、

前記中央演算装置は、
ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、
前記外部記録媒体や前記コンテンツ出力部と認証を行い、その成否を判断する認証成否判定部と、

前記認証成否判定部の判断からコンテンツの転送動作を有効化・無効化できる転送許可判定手段を有し、

前記中央演算装置が前記外部記録媒体・前記コンテンツ出力部のいずれかとの

間における第 1 の認証と、もう一方との間の第 2 の認証が連続して成功した場合に前記転送許可判定手段が肯定と判断して、前記命令実行部の制御に従ってコンテンツの転送が前記外部記録媒体と前記コンテンツ出力部の間で実行され、前記手段が否定と判断した場合に、前記命令実行部からの前記コンテンツの転送指示を指示通りに実行しないことを特徴とするコンテンツの転送装置。

【請求項 1 6】 暗号化されたコンテンツを蓄積する外部記録媒体と、前記コンテンツを出力するコンテンツ出力部と、前記外部記録媒体や前記コンテンツ出力部との認証や前記コンテンツの復号を行う中央演算装置を有する装置であって、

前記中央演算装置は、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

前記外部記録媒体から読み出した前記暗号コンテンツの復号処理を行う復号処理部と、

前記外部記録媒体や前記コンテンツ出力部と認証を行い、その成否を判断する認証成否判定部と、

前記認証成否判定部の判断からコンテンツの復号動作を有効化・無効化できる復号許可判定手段を有し、

前記中央演算装置が前記外部記録媒体・前記コンテンツ出力部のいずれかとの間における第 1 の認証と、もう一方との間の第 2 の認証が連続して成功した場合に前記復号許可判定手段が肯定と判断して、前記中央演算装置が前記外部記録媒体から読み出したコンテンツを復号した後、前記命令実行部の制御に従って前記コンテンツ出力部に転送し、前記手段が否定と判断した場合には前記復号や前記命令実行部の制御に従った転送を実行しないことを特徴とするコンテンツの復号・転送装置。

【請求項 1 7】 暗号化されたコンテンツを蓄積する外部記録媒体と、前記コンテンツを復号して出力するコンテンツ出力部と、前記コンテンツを転送する中央演算装置を有する装置であって、

前記中央演算装置は、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

前記暗号鍵を暗号する処理を実行する暗号鍵暗号部と、
前記暗号鍵を復号する処理を実行する暗号鍵復号部と、
前記外部記録媒体との間の共通鍵Aと前記コンテンツ出力部との間の共通鍵Bを格納する暗号鍵格納部を有し、
前記外部記録媒体は、前記コンテンツの暗号化に使用したコンテンツ鍵Cを前記共通鍵Aでさらに暗号化した形で格納しており、
前記中央演算装置は前記コンテンツ鍵Cを前記共通鍵Aを用いて前記暗号鍵復号部において復号した後、前記暗号鍵暗号部において、前記共通鍵Bで前記コンテンツ鍵Cを再度暗号化して、前記コンテンツ出力部へ転送する一方で、前記外部記録媒体から転送された暗号化されたコンテンツはそのまま前記コンテンツ出力部へ転送し、
前記コンテンツの暗号・復号の処理を省くことを特徴とするコンテンツの転送装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルコンテンツをセキュリティを保ちつつ復号と転送を実行する装置に関するものである。

【0002】

【従来の技術】

従来の構成における、コンテンツの復号・転送装置について図15を用いて説明する。

【0003】

図15は、外部記録媒体6に格納されている暗号化されたコンテンツを読み出し、復号した後に出力する装置を示したものである。データ保存部4はハードディスク、またはフラッシュメモリーのようにプログラムやユーザー・データを記録する書き換え可能な装置を表す。コンテンツ出力部2は、例えば圧縮されたマルチメディアデータの伸長処理やD/A変換の処理等の機能を含む、著作権コンテンツを装置外部に出力するモジュールを表す。

【 0 0 0 4 】

次に、外部記録媒体 6 の内部の暗号化されたコンテンツをコンテンツ出力部 2 から出力するまでの過程を説明する。ユーザーからコンテンツの復号要求が生じると、中央演算装置 1 は外部記録媒体認証部 8 に対して、外部記録媒体 6 を認証作業の開始を要求する。もし、認証が成立すれば、外部記録媒体インターフェース部 7 は、外部記録媒体 6 との間で決められたデータ転送プロトコルに応じて暗号化されたコンテンツを受信し、外部記録媒体認証部 8 に転送する。暗号化されたコンテンツは外部記録媒体認証部 8 で復号され、中央演算装置 1 の制御によって、システムバス 9 を介してコンテンツ出力部 2 に転送される。

【 0 0 0 5 】

システムバス 9 には汎用的な外部入出力インターフェース 5（例えば、USB など）が接続されている。ユーザーは、このインターフェース 5 を用いて、コンテンツを外部記録媒体 6 にダウンロードしたり、データ保存部 4 に保存しているソフトウェアを更新することが可能である。

【 0 0 0 6 】

また、図 1 5 の装置は図 1 6 のよう構成に変更することも可能である。つまり、外部記録媒体認証部 8 をコンテンツ出力部 2 とシステムバス 9 の間に配置する。この場合、暗号化されたコンテンツは外部記録媒体認証部 8 において復号されるため、システムバス 9 上では暗号化した状態のコンテンツのみが転送されることになる。

【 0 0 0 7 】

【発明が解決しようとする課題】

図 1 5 の装置において、システムバス 9 でのコンテンツの転送を制御するのは中央演算装置 1 である。中央演算装置 1 はデータ保存部 4 に格納されているソフトウェアに従って動作するが、この装置の場合、そのソフトウェアは外部入出力インターフェース部 5 を通じて更新可能である。そのため、もしユーザーが不正なコンテンツの取得を目的としてソフトウェアを改竄し、コンテンツの転送先を変更し外部入出力インターフェース部 5 から出力させることも可能となってしまう。このことは、著作権コンテンツの不正な複製につながるものであり、何らか

の形でこのようなソフトウェアの記述による中央演算装置 1 の動作を制限する必要がある。

【0008】

図 1 6 の構成は、ソフトウェアが転送するのは暗号化したコンテンツに限られるので、この観点では有効な手法である。しかし、コンテンツ出力部 2 が複数存在する場合には、コンテンツ出力部 2 の数だけ外部記録媒体認証部 8 が必要となり、その分実装が冗長となってしまう。特に、コンテンツ出力部 2 が複数種類存在する（例えば、音楽デコードDSP、画像デコードDSPなど）場合には、それぞれのインターフェースに合わせて外部記録媒体認証部 8 を変更する必要があるため、コンテンツ出力部 2 の種類に応じた実装工数が発生し、装置の構成としての汎用性に欠けるという問題がある。

【0009】

本発明は、上記に示した状況に鑑みてなされたものであり、中央演算装置に復号・認証の機能と外部ソフトウェア作成者の不正な意図に基づく動作を制限する機能を内蔵させることで、ソフトウェアを外部からダウンロードして自由に実行できる機能とコンテンツ復号装置としての汎用性を維持しつつ、コンテンツをセキュアに復号・転送できる装置を提供することを目的とする。

【0010】

【課題を解決するための手段】

本発明は、暗号化されたコンテンツを蓄積するデータ記録部と、暗号化されたコンテンツを復号する機能を有する中央演算装置と、復号されたコンテンツを出力するコンテンツ出力部を有する復号装置であって、

前記中央演算装置は、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

前記データ記録部から読み出した暗号データの復号処理を行う復号処理部と、

前記復号処理部で復号されたデータを格納する復号データ格納部と、

前記コンテンツ出力部のアドレスを含む、前記復号されたデータを転送しても良いアドレスを格納する転送先アドレス格納部と、

前記命令実行部が前記復号データ格納部に格納されているデータの転送を指示

した時、転送先のアドレスが前記転送先アドレス格納部に格納されているか否かを検査する転送是非判定部とを有し、

前記転送是非判定部は検査結果が否定である場合、命令実行部からの前記復号されたデータの転送指示を指示通りに実行しないことを特徴とする復号装置に関するものである。

【 0 0 1 1 】

また、復号機能を有する中央演算装置であって、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

暗号データの復号処理を2種類以上の暗号関数で実行する復号処理部と、

前記復号処理に用いる2種類以上の鍵を格納する暗号鍵格納部と、

2種類以上の暗号鍵、または2種類以上の暗号関数で暗号化された同一のデータの復号結果を前記復号処理部から入力してこれらと比較する比較手段を有し、復号結果が一致しないと前記比較手段が判定した場合、命令実行部からの復号されたデータの出力指示を指示通りに実行しないことを特徴とする中央演算装置に関するものである。

【 0 0 1 2 】

また、データの書き換えが可能なデータ記録部と、暗号・復号機能を有する中央演算装置とコンテンツ出力部を有する復号装置であって、

前記データ記録部は前記中央演算装置と前記コンテンツ出力部の間の共通鍵を暗号化した状態で記録する暗号化共通鍵記録部を有し、

前記中央演算装置は、

ソフトウェアの命令に従ってデータの転送等の処理を行う命令実行部と、

暗号化された暗号鍵を復号する暗号鍵復号部と、

復号された前記共通鍵や固定値の暗号鍵を格納する暗号鍵格納部とを有し、

前記コンテンツ出力部は、前記中央演算装置と同様に暗号化された暗号鍵を復号する暗号鍵復号部と、

復号された前記共通鍵や固定値の暗号鍵を格納する暗号鍵格納部とを有し、

前記共通鍵が前記中央演算装置と前記コンテンツ出力部の固定の鍵によって別々に暗号化された状態で前記データ記録部内の前記暗号化共通鍵記録部にあらか

じめ格納されていて、前記中央演算装置・前記コンテンツ出力部それぞれの前記暗号鍵復号部に転送・復号され、前記暗号鍵格納部に格納されることで共通鍵として設定され、前記データ記録部内の前記暗号化共通鍵記録部の内容の更新によって前記中央演算装置と前記コンテンツ出力部の間の共通鍵を更新することが可能なことを特徴とする装置に関するものである。

【 0 0 1 3 】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【 0 0 1 4 】

(実施の形態 1) 最初に本願発明に係わる、外部からダウンロードしたソフトウェアによる中央演算装置の不正なコンテンツ転送を防止する装置について説明する。図 1 は本願発明に係わるコンテンツ転送装置の全体図の一例を示した図であり、まずこの構成要素を説明する。コンテンツ出力部 2 や RAM 3、データ保存部 4、外部入出力インターフェース部 5、外部記録媒体 6、外部記録媒体インターフェース部 7 は、発明が解決しようとしている課題で述べた図 1 5 で説明したものと同様であるため、説明を割愛する。

【 0 0 1 5 】

命令実行部 1 0 1 は従来の中央演算装置に実装されている命令デコーダ・算術演算部・内蔵 RAM などを持ち、データ保存部 4 に格納されたソフトウェアはここで実行される。バス制御部 1 0 2 は中央演算装置 1 の内部バスやシステムバス 9 の制御を行うモジュールであり、命令実行部 1 0 1 が外部と入力・出力するデータはすべてバス制御部を通して転送される。

【 0 0 1 6 】

中央演算装置 1 は、暗号・復号処理を行う暗復号処理部 1 0 3 を内蔵している。図 2 は、図 1 における暗復号制御部 1 0 3 の構成を、鍵格納部 1 0 4、復号データ格納部 1 0 5、転送先アドレス格納部 1 1 2、認証成否判定部 1 1 3 との接続関係とともに詳細に示したものである。

【 0 0 1 7 】

暗復号処理部 1 0 3 の内部には暗号・復号の演算を実行する暗号演算回路 1 3

4と復号演算回路135が存在する。命令実行部101は、まず暗号演算回路134または復号演算回路135に実行させたい暗号・復号演算の命令を暗復号制御部133に入力する。暗復号制御部133は、入力した命令を解釈し、暗号演算回路134または復号演算回路135の入力データ、鍵、使用する暗号関数、演算結果の出力先を選択するモジュール、入力選択136、鍵選択138、関数選択139、出力選択137にそれぞれ出力する。入力選択136は選択回路131に入力している信号線（図では命令実行部101から、鍵格納部104から、乱数発生部140からの3種類）から暗号演算回路134または復号演算回路135の入力に接続すべきものを選択する。

【0018】

データ入力格納132は、演算回路134・135への入力するデータを一旦格納し、演算回路に入力できるデータの大きさにまとめてから、暗号演算回路134または復号演算回路135へ入力するモジュールである。例えばデータの入力先が命令実行部101であり命令実行部101が扱う1語が16ビット、暗号演算回路・復号演算回路の処理単位が64ビットであった場合には、データ入力格納132が命令実行部101の入力4回分をまとめて暗号演算回路134・復号演算回路135に入力する。同様に入力するデータが56ビットの鍵であった場合には、最上位または最下位の8ビットに冗長ビットを付加するなどの処理を行う。

【0019】

鍵選択138が出力した鍵選択信号は鍵格納部104に入力され、対応した鍵のデータが暗号演算回路134・復号演算回路135へ出力される。鍵格納部104の内部構成を図4に示しておく。入力データと鍵が選択されると、図2の暗復号制御部133は暗号関数（暗号演算回路134か復号演算回路135か）を選択し、演算が実行される。演算結果は出力選択137が指定する場所へ出力される。このような、暗復号制御部133の制御の流れを図6の(a)に示す。暗号演算回路134の出力結果は、中央演算装置1の内部バスを通して、命令実行部101に転送することが可能だが、復号演算回路135の出力結果は図2に示すように出力先が限定されている。

【 0 0 2 0 】

鍵格納部 1 0 4 は暗復号処理部 1 0 3 で用いられる鍵を格納するモジュールであり、鍵データを保存するレジスタへの入力、図 4 のように暗復号処理部 1 0 3 内の復号演算回路 1 3 5 の出力端子または乱数発生部 1 4 0 からのみ可能である。このため、鍵格納部内部の鍵情報を記録したレジスタの値を更新する場合には、図 1 の命令実行部 1 0 1 で実行されるソフトウェアによって、設定したい鍵の値を暗号化した状態で暗復号処理部 1 0 3 に入力しなければならない。また、鍵格納部 1 0 4 内のレジスタは、図 2 に示すように暗号演算回路 1 3 4 ・復号演算回路 1 3 5 の鍵入力端子またはデータ入力格納 1 3 2 にのみ出力可能であり、生の状態の鍵データが命令実行部 1 0 1 など暗復号処理部 1 0 3 以外のモジュールには転送されないようになっている。

【 0 0 2 1 】

ここで、以下の説明に用いる中央演算装置 1 固有の第 1 の鍵と第 2 の鍵について図 1 3 を用いて説明しておく。

【 0 0 2 2 】

第 1 の鍵は、暗復号処理部 1 0 3 で扱う機密情報を直接暗号化するのに用いる鍵である。この鍵は、暗復号処理部 1 0 3 での暗号・復号演算にのみ使用される鍵であり、他のモジュールの暗号演算回路・復号演算回路では使われない。図 1 3 の(a)に示すように、第 1 の鍵は、暗号と復号が同じ装置 4 0 1 内で実行される場合に用いられる鍵であり、装置 4 0 1 にユニークな値が用いられる（この意味で今後「～の固有の鍵」という言い方を用いる）。この値は暴露されないように、通常装置 4 0 1 の中で厳重に管理される。図 1 3 において、 $E()$ は暗号関数、 X は暗号化したいデータ、 Key_1 は第 1 の鍵、 Enc は暗号処理部、 Dec は復号処理部であることを示す。中央演算装置固有の第 1 の鍵は、例えば命令実行部 1 0 1 で実行されるソフトウェアの暗号化に用いたり、機密情報をデータ保存部 4 に（つまり、中央演算装置 1 の外部に）保存する場合に使用できる。

【 0 0 2 3 】

なお、前記第 1 の鍵は、上で述べたように機密情報を直接暗号化する鍵であり、これを固定値として鍵格納部 1 0 4 に実装して使い続けるのはセキュリティ上

好ましいことではない。そこで、鍵格納部 104 に第 2 の鍵を固定値として図 4 の第 2 の鍵格納 ROM 183 に固定値として ROM 実装し、この鍵を知る唯一の存在である中央演算装置 1 の開発者が、データ保存部 4 に第 1 の鍵を第 2 の鍵で暗号化して格納する。そして、暗号化された第 1 の鍵が暗復号制御部 103 に入力、第 2 の鍵で復号された後、鍵格納部 104 内に格納されることで、第 1 の鍵が設定される。中央演算装置 1 の開発者が第 1 の鍵を更新したいと考えた際は、データ保存部 4 に格納しておく、第 2 の鍵で暗号化された第 1 の鍵のデータを更新すればよい。このことを図 13 の (b) に示す。(a) における Key1 を保護するために装置 401 の固定鍵である Key2 を利用し、Key2 で暗号化した Key1 を装置 401 の外部の書き換えできる場所に保存しておけばよい。

【0024】

命令実行部 101 が暗復号処理部 103 へ暗復号処理の内容と暗復号したいデータを設定する手順はあらかじめ決められており、図 2 の暗復号制御部 133 中のステートマシンとして実装されている。ステートマシンの一例を図 6 の (b) (c) に示す。ステートマシンにおけるそれぞれの状態には暗復号処理部 103 が実行できる命令と実行できない命令が存在する。例えば、初期化の後には第 1 の鍵設定の命令以外は、いかなる命令が命令実行部 101 から暗復号制御部 133 に入力されても、暗復号制御部 133 はこれを受け付けない。これによって、所定の手順で命令実行部が暗復号制御部 133 にデータを入力しているかが判断される。(b)、(c) それぞれのステートマシンの意義については後述する。ステートマシン上の状態で実行可能な命令が入力された場合には、暗復号制御部 133 は命令内容をデコードして、前述の入力選択 136 や鍵選択 138、関数選択 139、出力選択 137 に、命令に対応した選択信号を出力し、暗復号演算を実行させる。実行できない命令の場合には、前記の選択モジュールから選択信号は出力されず、暗号・復号演算は実行されない。

【0025】

図 1 の復号データ格納部 105 は暗復号処理部 103 で復号されたデータ（コンテンツなど）を格納するモジュールであり、格納されたデータは転送先アドレス検査部 111 にのみ出力される。

【0026】

図1の転送先アドレス格納部112は、復号データ格納部105内に格納されているデータが転送されるべき行き先のアドレス範囲を格納したモジュールである。ここに格納されているデータはハードウェア的な固定値として実装されていても、レジスタとして可変にできるように実装されていてもよい。ただし、後者の場合、そのレジスタへの入力には暗復号処理部103内部の復号演算回路135からのみ可能であり、命令実行部101で実行されるソフトウェアによって、鍵格納部104に格納されている中央演算装置1固有の第1の鍵で暗号化された状態で暗復号制御部133に入力しない限り、転送先アドレス範囲を更新できない。

【0027】

転送先アドレス検査部111の構成を図3に示す。命令実行部101は、転送先設定格納161のレジスタのアドレスを指定し、転送先設定格納161に復号データ格納部105のデータ転送先のアドレスを格納する。その時、被選択判定162は、中央演算装置1内部のアドレスバスが前記転送先設定格納161のレジスタを指定していることを検知すると同時に、enable信号を比較回路163に出力する。比較回路163では、enable信号が肯定された際、転送先設定格納161に設定された転送先アドレスが転送先アドレス格納部112で指定されているアドレス範囲に含まれているかどうかを判定する。比較回路163が肯定の判定を出力した場合、バス使用制御164は命令実行部101にバスの使用权を要求する信号を出力する。転送先設定格納161に書き込まれたアドレスはアドレス出力165に、復号データ格納部105内に格納されている復号化データはデータ出力166に接続されており、バス使用制御164がバスの使用权を得た際に、それぞれアドレスライン、データラインにWE信号とともに出力される。

【0028】

図1の認証成否判定部113は、図14に示した対話認証プロトコルという方法に基づいて、認証処理を行うモジュールである。図14において501と502はあらかじめ共通鍵510を共有しており、501は502が自分と同一の共通鍵を所有していると判断した際に、501は502を認証したと判断する。

【0029】

まず、501は502に乱数521を送信し、502はその乱数を自分の持っている共通鍵510で暗号化したデータ522を返信する。501は乱数521を自分の持っている共通鍵510で暗号化したデータ523が522と同じかどうか比較し、もし同じであれば501は502が自分と同じ共通鍵を所有していると判断できる。このような乱数を用いた認証の方法は、乱数に応じて妥当な値を返答する必要があるため、共通鍵そのものを知らない限り常に成功させることは困難であり、不正なモジュールを排除する手法としてよく用いられている。

【0030】

この認証成否判定部113の内部構成は図5のようになっており、暗復号処理部103で暗号化された共通鍵を暗号化乱数格納部171に、認証対象において暗号化され返答されてきたデータを返答格納部172に格納する。返答格納部172と暗号化乱数格納部171に格納されたデータは比較回路173で比較され、それらが等しければ認証が成功したと判断し、暗復号制御部133にその結果を出力する。

【0031】

図2の乱数発生部140は、暗復号制御部133から入力選択136を通して乱数発生の要請があった場合に、乱数を出力するモジュールである。乱数の出力先は用途によって異なる。新たな鍵データを生成するのに用いられる場合の出力先は鍵格納部104である。図14のような認証に用いられる場合、まず選択回路131に入力され、暗号化された後、内部バスを通じて命令実行部101に出力され、その後認証対象へ送信される。

【0032】

次に図1における、外部記録媒体6から転送されてきたコンテンツをコンテンツ出力部2へ転送する際の動作を説明する。外部記録媒体インターフェース7から入力された暗号化コンテンツは、命令実行部101におけるデータ転送命令の実行により、RAM3もしくは命令実行部101内の内蔵RAMを経由して、暗復号処理部103へ転送される。暗復号処理部103はコンテンツを復号し、その結果を復号データ格納部105へ出力する。転送先アドレス格納部112には、コン

テンツ出力部 2 と中央演算装置 1 内の暗復号処理部 1 0 3 内のレジスタに該当するアドレス範囲が登録されている。命令実行部 1 0 1 は、コンテンツの正規の転送先であるコンテンツ出力部 2 に対応するアドレスを転送先アドレス検査部 1 1 1 内部の転送先設定格納 1 6 1 (図 3) に設定する。そのアドレスが転送先アドレス格納部 1 1 2 で指定されているアドレス範囲に含まれていることが比較回路 1 6 3 において確認された場合、復号化されたコンテンツは、データ出力 1 6 6 からコンテンツ出力部 2 へ出力される。

【 0 0 3 3 】

命令実行部 1 0 1 が転送先設定格納 1 6 1 に設定したアドレス値が外部入出力インターフェース部 5 に対応するものであった場合には、比較回路において転送先アドレス格納部 1 1 2 で設定されてあるアドレス範囲にないと判定され、バス使用制御 1 6 4 はバス使用権要求信号を出力せず、復号データ格納部 1 0 5 内に格納されている復号化されたコンテンツは転送されない。

【 0 0 3 4 】

なお、以上の動作は、暗号化されたコンテンツが外部入出力インターフェース部 5 を通じて外部から入力される場合においても同様である。

【 0 0 3 5 】

なお、図 3 の転送先アドレス検査部の説明で、バス使用制御 1 6 4 が命令実行部 1 0 1 からバスの使用権を受け取り、データを転送する形式を採った。しかし、命令実行部 1 0 1 で実行される命令語レベルで、復号データ格納部 1 0 5 からデータを読みとり命令実行部 1 0 1 内の汎用レジスタ以外の特別な領域に一旦格納する動作を行う特別なものをサポートさせ、そのデータの出力先アドレスを監視する機構を命令実行部 1 0 1 内部に設けたとしても、本願発明と論理的に同等である。

【 0 0 3 6 】

なお、図 2 の暗復号制御部 1 3 3 に命令実行部 1 0 1 が入力する命令も、暗号化した方がセキュリティを高めることができる。これを実現するためには、上記の装置を以下のように動作させればよい。つまり、命令実行部 1 0 1 は暗復号処理命令を中央演算装置固有の第 1 の鍵で暗号化した状態で、暗復号処理部 1 0 3

内のデータ入力格納132に入力し、復号演算回路135で復号させる。そして、復号化された命令を復号データ格納部105にバッファし、そのデータの転送先アドレスを指定する転送先設定格納161に、暗復号制御部133の命令入力レジスタに相当するアドレスを設定する。このアドレスが、転送先アドレス格納部112に格納されているアドレス範囲に含まれるように、アドレス範囲を設定しておけば、暗復号制御部133に復号化された命令を入力することができる。

【0037】

なお、暗復号制御部133に実装するステートマシンを図6(b)のように設定し、前記第1の鍵や転送先アドレス範囲の設定の過程を経ないと、認証・コンテンツ転送を行わないようにしておくと、初期化の際に第1の鍵や転送先アドレス範囲が未設定のまま、ソフトウェアによって不正なコンテンツ転送が実行されるのを防ぐことができる。

【0038】

なお、図1では外部記録媒体インターフェース部7が中央演算装置1の外部に配置するように示してあるが、これを図7の外部記録媒体インターフェース部121のように中央演算装置1と一体化する形態であっても本願発明の内容には影響はない。

【0039】

(実施の形態2) 次に、本願発明に係わる、ソフトウェアによる暗復号処理回路への不正な設定を防止する装置について述べる。既に図1の暗復号処理部103の構成の一例として説明した図2に記載されている暗復号処理部103を図8に記載のものに変更したものが、本願発明に係わるコンテンツ転送装置の一例である。

【0040】

この装置の目的は、正規のソフトウェアを改竄して作成した不正なソフトウェアが、第1の鍵の値を正確に把握していない限り、正規のソフトウェアと異なる設定を実行することを困難にすることである。図9(a)(b)に示すように、ソフトウェアを用いてある値を設定させたい場合(図9ではAで示してある)、その値を2種類以上に暗号化した状態で設定させ、その2つ以上の値の復号結果に矛盾

がないかどうかを調べることで、正規のソフトウェアによる設定か否かを判断することが、動作の概要である。

【 0 0 4 1 】

そのための仕組みについて、図 8 を用いて説明する。図 2 と共通の部分については説明を割愛する。

【 0 0 4 2 】

復号演算回路 1 と復号演算回路 2 は入力する鍵と暗号データのビット長の仕様は同じであるが、用いる暗号関数が異なる回路である。例えば、同じ DES 暗号 (Data Encryption Standard) のアルゴリズムを用いて、その暗号関数のパラメータである S ボックスの値を 2 通りに用意する、という方法が考えられる。

【 0 0 4 3 】

比較回路 1 4 1 は復号演算回路 1 3 5 1 と復号演算回路 1 3 5 2 の出力を比較し、もし等しければ出力選択 1 3 7 に enable 信号を出す。出力選択 1 3 7 は、enable 信号が有効の場合のみ復号データの出力先選択信号を出力することができる。

【 0 0 4 4 】

次にこの装置において、命令実行部 1 0 1 が、上記で説明済みの転送先アドレス範囲を設定する場合を例に、その動作を説明する。

【 0 0 4 5 】

データ保存部 4 に格納されている正規のソフトウェアには、設定値を 2 種類の関数を用いて暗号化された値が、ソフトウェア開発者によって実装されている。まず、命令実行部 1 0 1 は、転送先アドレス範囲の設定処理を行う命令を図 8 の暗復号制御部 1 3 3 に入力する。その後、2 種類に暗号化された設定値を、順に図 8 のデータ入力格納 1 3 2 に入力する。これらは、復号演算回路 1 3 5 1、復号演算回路 1 3 5 2 でそれぞれ復号され、その結果が比較回路に出力される。正規のソフトウェアによる設定の場合には、比較回路 1 4 1 は 2 つの復号結果が等しいことから、出力選択 1 3 7 に enable 信号を出力する。出力選択 1 3 7 は enable 信号が有効であることから、暗復号制御部 1 3 3 から入力する暗復号命令の情報を基に、転送先アドレス格納部 1 1 2 を指定し、復号された結果はそこに転送

される。

【0046】

不正ソフトが正規ソフトウェアを改竄し、転送先アドレス範囲を変更しようとする場合、不正ソフトウェアは正規ソフトウェアと同様に、転送先アドレス範囲を2種類に暗号化した状態で設定する必要がある。しかし、2種類の関数を知らない限り比較回路141で等号が成立させることができないため、出力選択137は出力先選択信号を出力せず、復号化された不正な転送先アドレス範囲は転送されない。

【0047】

なお、図9(b)のように、暗号関数でなく鍵を2種類用意し、2通りに暗号化されたデータを入力させる方法も可能である。この場合、鍵を切り替えて用いるようにすれば、図8で2つ存在する復号演算回路は1つで十分であり、比較回路141で比較される復号結果を格納するレジスタが2つあればよい。

【0048】

なお、暗号関数や鍵を3種類以上実装する方法も上記と同様に可能である。ただしこの場合、比較回路141で比較される復号結果を格納するレジスタは高々2つあれば十分である。というのは、たとえ3個以上の復号データがあったとしても、それらを前記2つのレジスタへ交互に入力し、その都度比較回路で等号が成り立つかを調べることにすれば、そのいずれの場合でも等号が成立し続けなければならないからである。

【0049】

この方法を用いれば、比較回路141で等号が成立しなかった時点でソフトウェアが正規のものでないことが判明するので、比較回路141が否定の判断を下した際に装置全体を初期化しソフトウェアに初期設定からやり直すことを要求する、またはデータ保存部4に保存してあるプログラムを異なるものに更新することを要求する、または乱数発生部140から乱数を鍵格納部104に入力して中央演算装置固有の第1の鍵を新しい値に設定し直し、データ保存部4に保存してあるプログラムをその新しい第1の鍵で暗号し直すことを要求する、などの処理を行うようにすれば鍵の総当たり攻撃の手間を大幅に増大させることができる。

【 0 0 5 0 】

(実施の形態 3) 次に、本願発明に係わる、共通鍵暗号で用いる共通鍵を安全に共有・更新する装置について述べる。

【 0 0 5 1 】

コンテンツの転送に関わるモジュール毎に認証機能を持つ暗復号処理部を持たせる場合、そのモジュールの間で鍵を設定する必要がある。その鍵として永久に同じ値の共通鍵を使用し続ける場合、共通鍵が暴露された際に甚大な被害を被ることになる。そのため、コンテンツの転送に長期間にわたる安全性を持たせるためには、鍵の値を安全に更新できる機構を持つことが望ましい。

【 0 0 5 2 】

この装置は、共通鍵の値を安全に更新するための仕組みとして、図 1 のコンテンツ出力部 2 にも認証・暗復号の機能を持たせた図 1 0 のような構成を持つ。コンテンツ出力部 2 の内部構成は、図 1 1 に示している。

【 0 0 5 3 】

まず、この装置で実行される共通鍵の生成処理の概要について図 1 2 を用いて説明する。

【 0 0 5 4 】

中央演算装置 1 とコンテンツ出力部 2 には共に、それぞれの固有の鍵を固定値として実装されている。図 1 2 では中央演算装置 1 固有の固定鍵を K_{cpu} 、コンテンツ出力部 2 固有の固定鍵を K_{cont} で示している。中央演算装置 1 とコンテンツ出力部 2 の間の共通鍵の初期値 K_0 は、 K_{cpu} と K_{cont} で暗号化された状態 $f(K_0, K_{cpu})$ 、 $f(K_0, K_{cont})$ で、それぞれデータ保存部 4 に格納されている ($f(d, k)$: 暗号関数、 d : データ、 k : 鍵)。この 2 つの暗号化された共通鍵の初期値は、それぞれ中央演算装置 1、コンテンツ出力部 2 に転送されて復号化され、共通鍵の初期値 K_0 に復号される。この仕組みを用いれば、中央演算装置 1 とコンテンツ出力部 2 の固有の鍵 K_{cpu} 、 K_{cont} を知る唯一の存在である装置開発者がデータ保存部 4 に格納する $f(K_0, K_{cpu})$ 、 $f(K_0, K_{cont})$ の値を変更することで、共通鍵の初期値 K_0 を更新することができる。

【 0 0 5 5 】

続けて、中央演算装置 1 は、乱数発生装置から乱数 R1 を取り出し新しい共通鍵 K1 とする。この K1 は、中央演算装置 1 の暗復号処理部 1 0 3 において現在の共通鍵 K0 で暗号化された後、コンテンツ出力部 2 に転送され、コンテンツ出力部 2 で復号されることで、新しい K1 が中央演算装置 1 とコンテンツ出力部 2 の間で共有される。以下、共通鍵を用いたアクセスがある毎に共通鍵を更新していくようにすれば、同一の共通鍵を用い続けることによる危険性を完全に避けることが可能となる。

【 0 0 5 6 】

次に図 1 1 の構成要素について説明する。バスインターフェース 2 0 1 は、中央演算装置 1 とシステムバスを通じてデータの送受信を行うモジュールであり、暗号・復号の対象となるデータはデータ入力格納 2 0 2 へ、暗号・復号の制御信号は暗復号制御部 2 0 3 へ、中央演算装置 1 との認証時に用いられるデータは認証成否判定部 2 0 6 へ転送される。

【 0 0 5 7 】

暗復号制御部 2 0 3 は中央演算装置 1 から入力した命令内容から、暗復号演算部 2 0 4 で実行されるべき処理内容を判断し、暗号・復号演算の入力データをデータ入力格納 2 0 2 や乱数発生部 2 0 7、鍵格納部 2 0 5 の中から選択する。その後、鍵を鍵格納部 2 0 5 から選択して、暗復号演算部 2 0 4 で演算を実行させ、演算が終了した場合にはその出力先をコンテンツ伸長部 2 0 8 または鍵格納部 2 0 5 または認証成否判定部 2 0 6 の中から指定する。

【 0 0 5 8 】

鍵格納部 2 0 5 は暗復号演算部 2 0 4 で用いられる鍵を格納するモジュールであり、図 1 における鍵格納部 1 0 4 と同様、ここに格納される鍵の情報は暗号・復号演算を介した形でなければ命令実行部 1 0 1 からアクセスできないようになっている。

【 0 0 5 9 】

認証成否判定部 2 0 6 は、図 1 の認証成否判定部 1 1 3 と同様に、図 1 4 のような乱数を用いた認証を実行するためのモジュールである。

【 0 0 6 0 】

コンテンツ伸張部 2 0 8 は、暗復号演算部 2 0 4 で復号された圧縮コンテンツを伸張するモジュールである。D/A 2 0 9 はコンテンツ伸張部 2 0 8 が出力したデジタルコンテンツをアナログ信号に変換して出力する。

【 0 0 6 1 】

次に図 1 0 の装置の、図 1 2 に即した動作について説明する。中央演算装置 1、コンテンツ出力部 2 固有の固定鍵はそれぞれ鍵格納部 1 0 4、2 0 5 にあらかじめ格納されている。命令実行部 1 0 1 は、データ保存部 4 から暗号化された共通鍵 $f(K0, K_{cpu})$ 、 $f(K0, K_{cont})$ を読み出し、中央演算装置 1 内部の暗復号処理部 1 0 3 とコンテンツ出力部 2 のデータ入力格納 2 0 2 へ転送する。次に命令実行部 1 0 1 は、共通鍵の初期値を演算する命令を双方の暗復号制御部 1 3 3 と 2 0 3 に入力し、暗復号制御部 1 3 3・2 0 3 の制御により中央演算装置 1 とコンテンツ出力部 2 双方において共通鍵 $K0$ が算出され、鍵格納部 1 0 4、2 0 5 に格納される。

【 0 0 6 2 】

次に、命令実行部 1 0 1 が共通鍵更新命令を中央演算装置 1 内部の暗復号処理部 1 0 3 に入力すると、乱数生成部 1 4 0 で生成した乱数が鍵格納部 1 0 4 に新しい共通鍵 $K1$ として格納される。その後、暗号演算回路 1 3 4 において現在の共通鍵 $K0$ で暗号化され、その結果はそのまま命令実行部 1 0 1 の制御により、コンテンツ出力部 2 へ送信される。

【 0 0 6 3 】

命令実行部 1 0 1 は共通鍵更新命令を暗復号制御部 2 0 3 にも入力し、暗復号制御部 2 0 3 の制御によって現在の共通鍵 $K0$ が鍵格納部 2 0 5 から暗復号演算部 2 0 4 へ呼び出される。これにより、中央演算装置 1 から転送された暗号化された新しい共通鍵 $K1$ が暗復号演算部 2 0 4 で復号され、その後鍵格納部 2 0 5 に格納される。以上により、中央演算装置 1 とコンテンツ出力部 2 の間で新しい共通鍵 $K1$ が共有化される。

【 0 0 6 4 】

なお、図 1 2 では乱数 $R1$ の値をそのまま新しい共通鍵 $K1$ として使用しているが、例えば共通鍵 $R1$ と $K0$ の排他的論理和を用いる、など何らかの演算を用いること

も可能である。

【 0 0 6 5 】

なお、次々に更新されていく共通鍵を不揮発性のメモリに格納しておけば、更新された状態での共通鍵のデータを電源が入っていない状態でも保管できるため、一度使用された共通鍵は二度と用いることがないようにすることが可能であり、セキュリティを高める上で効果がある。

【 0 0 6 6 】

（実施の形態 4）次に、本願発明に係わる、一旦認証に成功しても連続する認証に失敗した際にデータ処理量を増大させることによりセキュリティを向上させる装置について説明する。この装置の一例として、図 1 0 および図 2 を用いて説明する。ただしこの装置においては、中央演算装置 1 とコンテンツ出力部 2、外部記録媒体 6 とは共通鍵であり、さらに図 2 の暗復号制御部 1 3 3 に実装されるステートマシンは図 6（c）に示すものである。図 6 の (b) と (c) の違いは、外部記録媒体 6 との認証が成功した後に、続けてコンテンツ出力部 2 との認証を成功させなければ、コンテンツの復号（コンテンツ鍵の復号を含む）を実行しないようにした点である。中央演算装置 1 やコンテンツ出力部 2、外部記録媒体 6 が正規のモジュールである場合、これらの間の共通鍵が正確に実装されているので、図 6 (c) のように外部記録媒体 6 やコンテンツ出力部 2 との認証を連続して実行しても図 1 4 のような乱数を用いた認証で失敗することはない。

【 0 0 6 7 】

次に、復号済みコンテンツを不正に取得したい者がコンテンツ出力部 2 を正規でないものに置き換えた場合について説明する。不正なコンテンツ出力部 2 のモジュールは共通鍵が未知のため、共通鍵を総当たりで 1 つ 1 つ試していき、図 1 4 のような乱数を用いた認証において成功するまで何度も繰り返す必要がある。しかし一度、認証に失敗すると、図 6 (c) のステートマシンの制御により、再度、中央演算装置 1 の初期設定、外部記録媒体 6 との認証から始める必要があるため、共通鍵を暴くための鍵の総当たり攻撃にかかる時間が増大し、セキュリティを高めることができる。

【 0 0 6 8 】

(実施の形態5) 次に、本願発明に係わる、コンテンツの暗号の演算量を減少させる装置について説明する。この装置の構成は図10に示したものと同一である。

【0069】

まず、この装置の説明に用いる鍵について図13(b)を用いて説明する。コンテンツを暗号化して転送する場合、(b)の図に示すように、コンテンツを直接暗号化するKey4を共通鍵Key3で暗号化して、暗号化したコンテンツと一緒に転送する。以下、Key3を共通鍵、Key4をコンテンツ鍵と呼ぶ。暗号化して転送されたコンテンツ鍵はコンテンツ受信側で復号され、暗号化したコンテンツを復号するのに用いられる。

【0070】

この装置の目的は、コンテンツを外部記録媒体6から中央演算装置1を経由して、システムバス9上でも暗号化した状態でコンテンツ出力部2へ転送する際に、中央演算装置1でコンテンツを復号、そして再度暗号する作業を除去し、演算量を減少させることである。

【0071】

この装置の動作を図10を用いて説明する。図10の暗復号処理部103の構成は図2と共通であるため、詳細な説明を省略する。共通鍵は中央演算装置1と外部記録媒体6の間、中央演算装置1とコンテンツ出力部2の間のそれぞれに設定され、図10の中央演算装置1やコンテンツ出力部2や外部記録媒体6の鍵格納部に保管されている。以下、前者の共通鍵を第1の共通鍵、後者を第2の共通鍵と呼ぶ。外部記録媒体6から転送された暗号化コンテンツは命令実行部101の制御によって、中央演算装置1での暗号・復号の処理を一切受けず、コンテンツ出力部2へそのまま転送される。一方、第1の共通鍵で暗号化されたコンテンツ鍵は中央演算装置1内部の復号演算回路135で一旦復号され鍵格納部104へ格納される。その後、データ入力格納132を通して暗号演算回路134に入力され、第2の共通鍵で暗号化し直された後、命令実行部101の制御によってコンテンツ出力部2へ転送される。

【0072】

このようにすると、中央演算装置 1 における、データ量の多いコンテンツの暗号・復号の演算量を完全に削除することができる。

【0073】

【発明の効果】

以上のように、本発明によると、ユーザーが任意の外部プログラムをダウンロードして実行できる機能を維持しつつ、外部プログラムによる中央演算装置の不正な動作を制限することが、従来の中央演算装置の構造を根本的に変更すること無しに、実現することが可能である。また、中央演算装置に接続したバス上のコンテンツをセキュリティを保ちつつ転送することが可能である。

【図面の簡単な説明】

【図 1】

コンテンツ転送装置の一例を示す図

【図 2】

暗復号処理部の構成を示す図

【図 3】

転送先アドレス検査部の構成の一例を示す図

【図 4】

鍵格納部の構成を示す図

【図 5】

認証成否判定部の構成を示す図

【図 6】

暗復号制御部に実装する制御の例を示す図

【図 7】

コンテンツ転送装置の一例を示す図（外部記録媒体インターフェースが中央演算装置の内部にある場合）

【図 8】

不正設定を防止する装置における暗復号処理部の構成を示す図

【図 9】

不正設定を防止する装置における処理内容の概要を示す図

【図 1 0】

コンテンツ転送装置の一例を示す図

【図 1 1】

コンテンツ出力部の構成を示す図

【図 1 2】

共通鍵の生成・更新方法を示す図

【図 1 3】

鍵の補足説明に用いる図

【図 1 4】

乱数を用いた対話認証プロトコルの内容を示す図

【図 1 5】

従来のコンテンツ転送装置の一例を示す図（外部入出力がない場合）

【図 1 6】

従来のコンテンツ転送装置の一例を示す図（外部入出力がある場合）

【符号の説明】

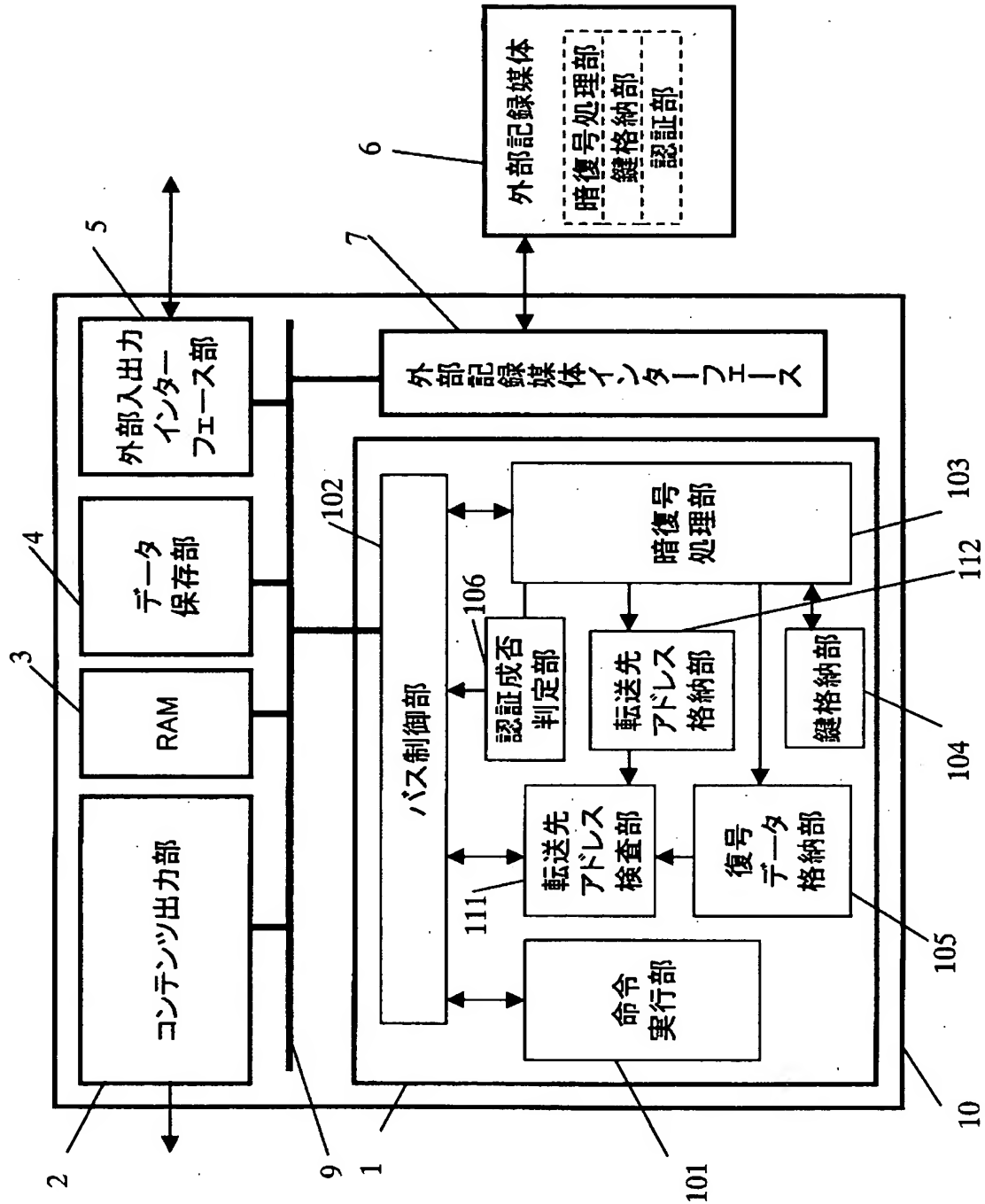
- 1 中央演算装置
- 2 コンテンツ出力部
- 3 RAM(Random Access Memory)
- 4 データ保存部
- 5 外部入出力インターフェース部
- 6 外部記録媒体
- 7 外部記録媒体インターフェース部
- 8 外部記録媒体認証部
- 9 システムバス
- 1 0 コンテンツ転送装置
- 1 0 1 命令実行部
- 1 0 2 バス制御部
- 1 0 3 暗復号処理部（中央演算装置内）
- 1 0 4 鍵格納部（中央演算装置内）

- 1 0 5 復号データ格納部
- 1 1 1 転送先アドレス検査部
- 1 1 2 転送先アドレス格納部
- 1 1 3 認証成否判定部
- 1 2 1 外部記録媒体インターフェース部
- 1 3 1 選択回路
- 1 3 2 データ入力格納
- 1 3 3 暗復号制御部
- 1 3 4 暗号計算回路
- 1 3 5 復号演算回路
- 1 3 5 1 復号演算回路 1
- 1 3 5 2 復号演算回路 2
- 1 3 6 入力選択
- 1 3 7 出力選択
- 1 3 8 鍵選択
- 1 3 9 関数選択
- 1 4 0 乱数発生部
- 1 6 1 転送先設定格納
- 1 6 2 被選択判定
- 1 6 3 比較回路
- 1 6 4 バス使用制御
- 1 6 5 アドレス出力
- 1 6 6 データ出力
- 1 7 1 暗号化乱数格納部
- 1 7 2 返答格納部
- 1 7 3 比較回路
- 1 8 1 入力元選択
- 1 8 2 鍵格納レジスタ
- 1 8 3 第 2 の鍵格納ROM

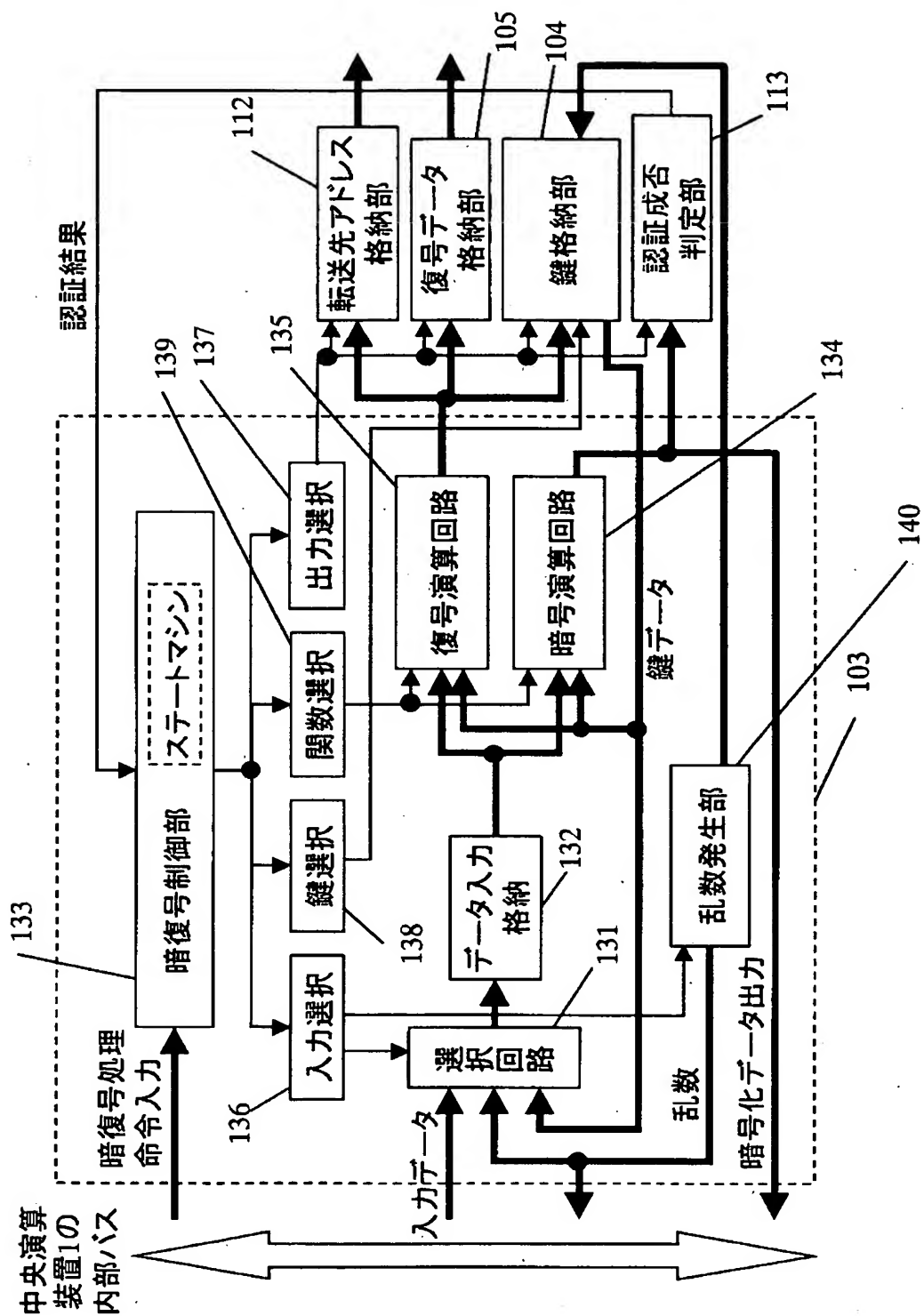
- 1 8 4 出力鍵選択
- 2 0 1 バスインターフェース部
- 2 0 2 データ入力格納
- 2 0 3 暗復号制御部
- 2 0 4 暗復号演算部
- 2 0 5 鍵格納部
- 2 0 6 認証成否判定部
- 2 0 7 乱数発生部
- 2 0 8 コンテンツ伸張部
- 2 0 9 D/A
- 4 0 1 固有の鍵を持つ暗号・復号装置
- 4 0 2 コンテンツ転送元
- 4 0 3 コンテンツ転送先
- 5 0 1 認証者
- 5 0 2 被認証者
- 5 1 0 共通鍵
- 5 2 1 乱数
- 5 2 2 返答
- 5 2 3 認証者が暗号化した乱数

【書類名】 図面

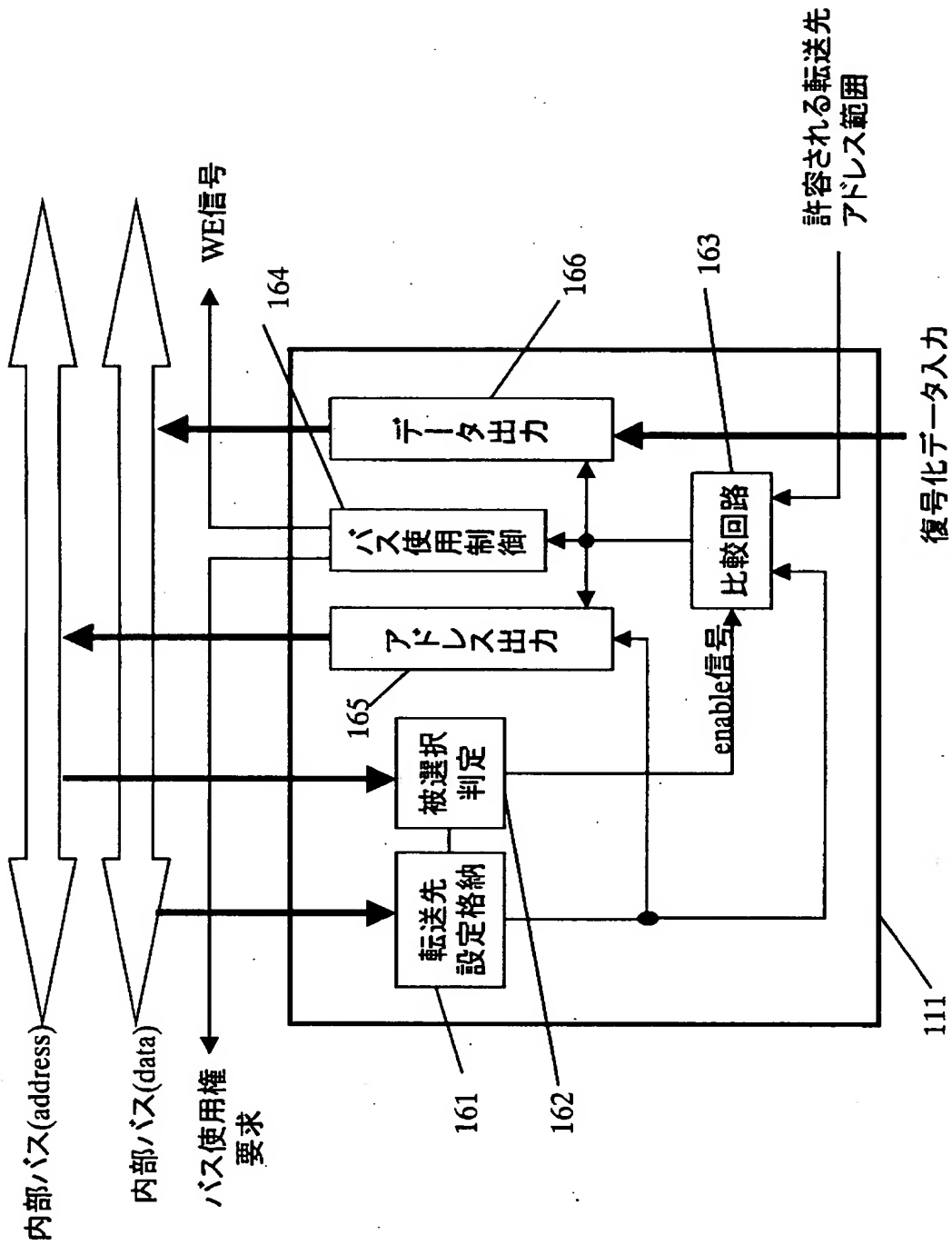
【図 1】



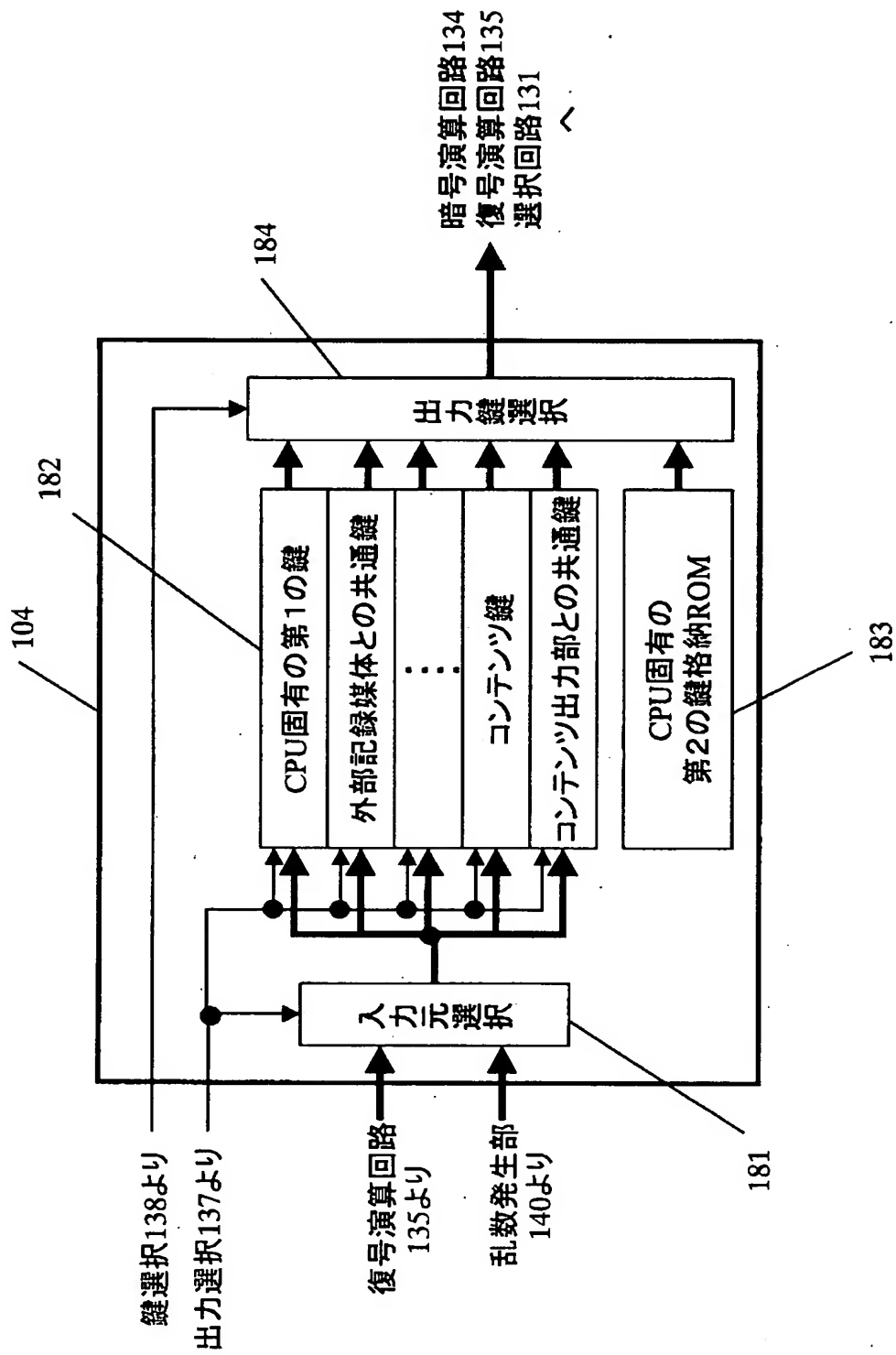
【図 2】



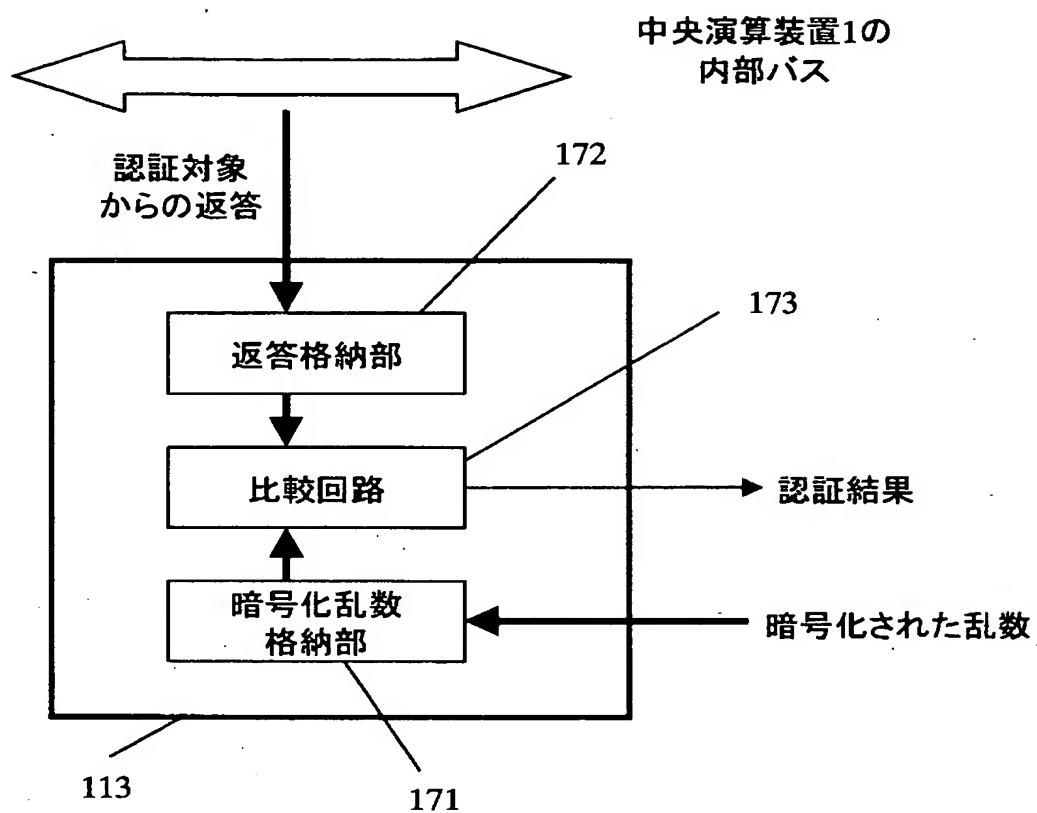
【図3】



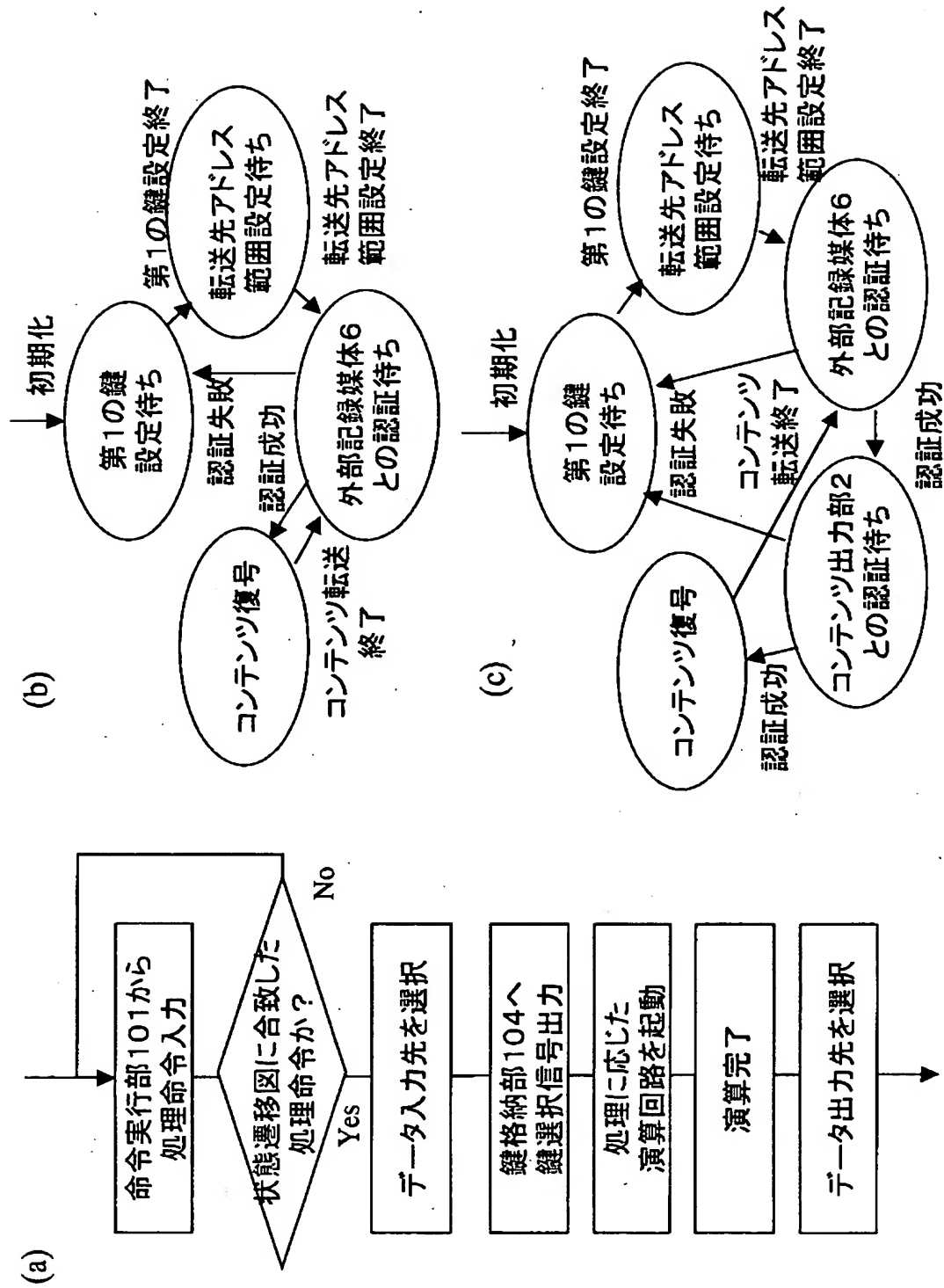
【図 4】



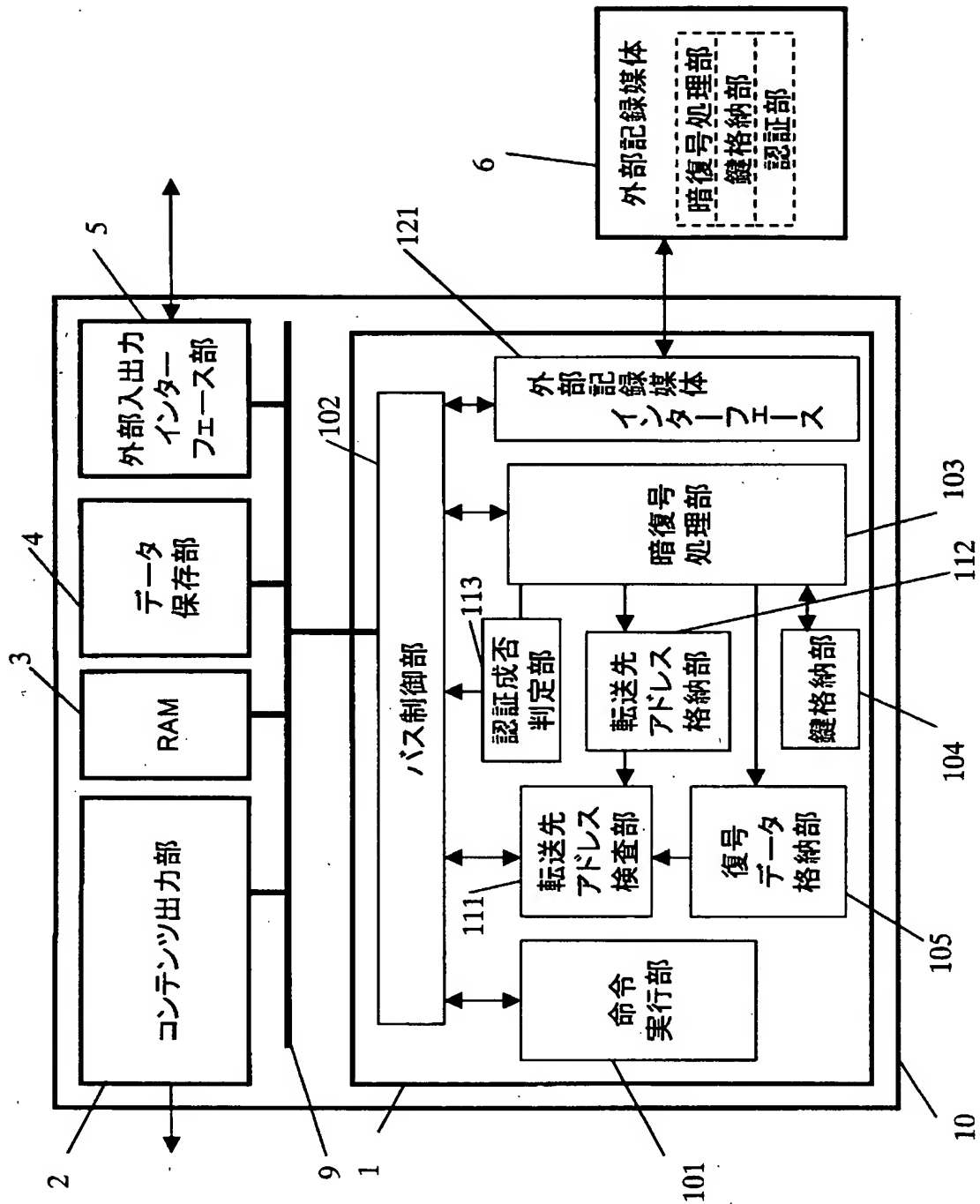
【図 5】



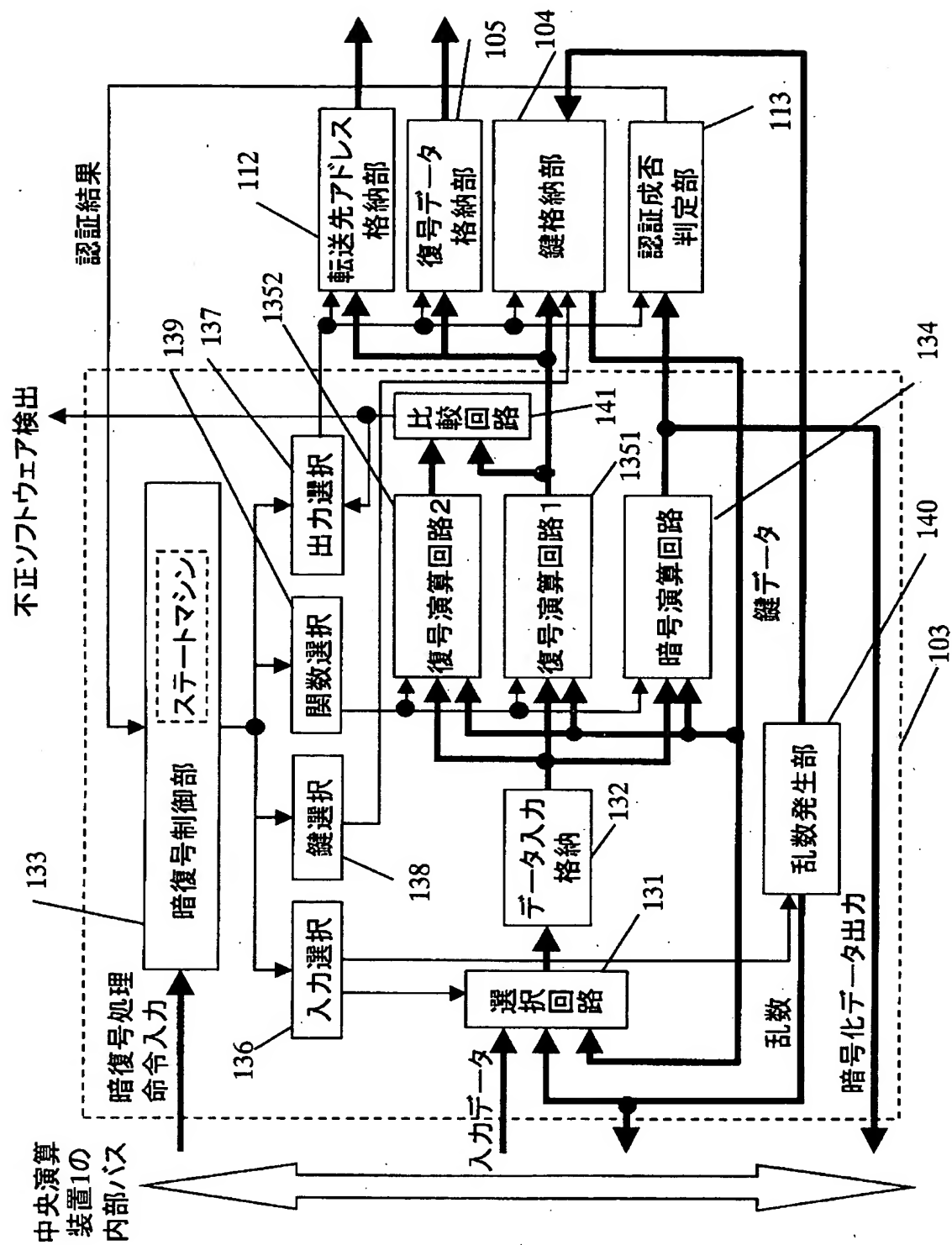
【図6】



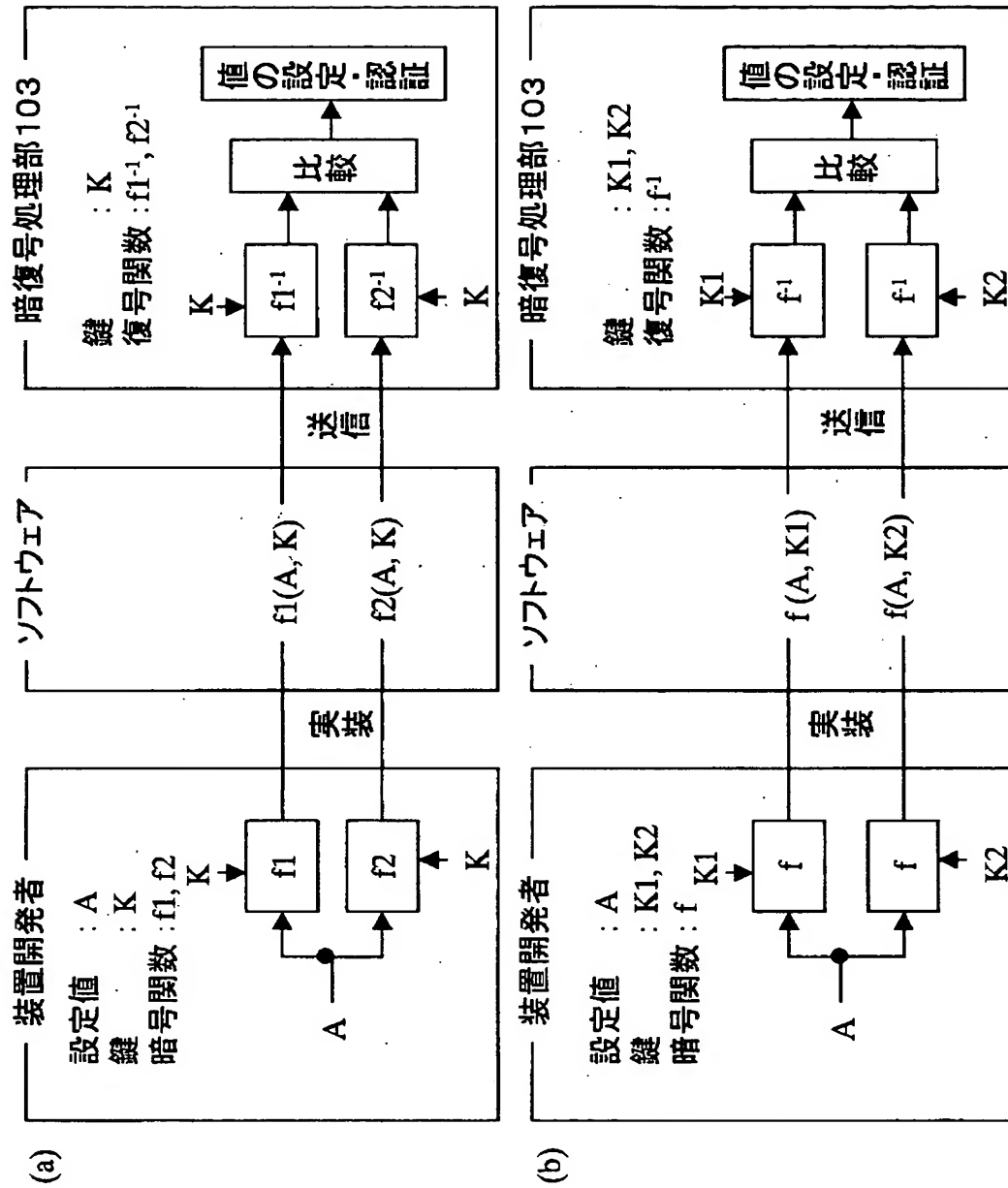
【図 7】



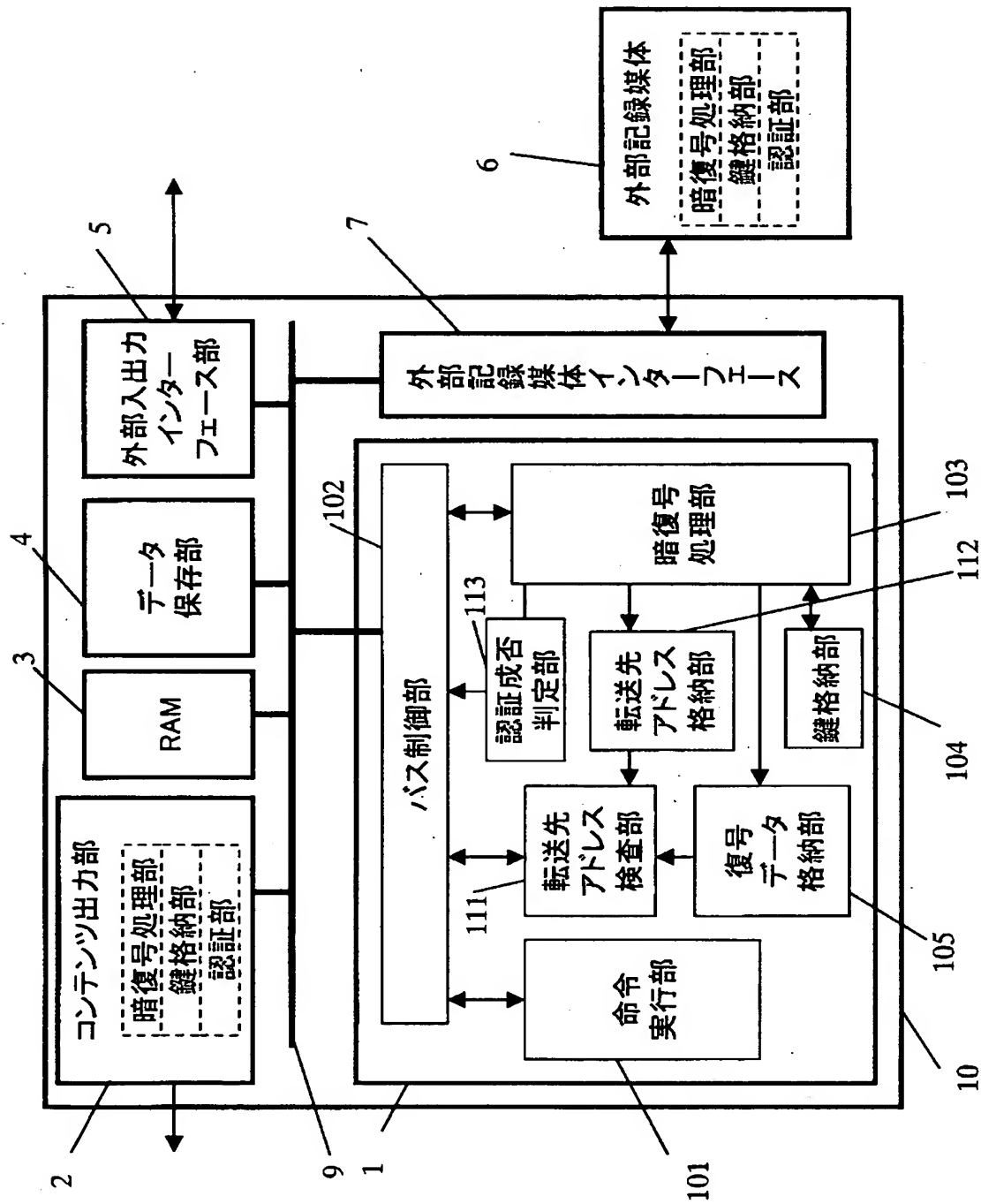
【図 8】



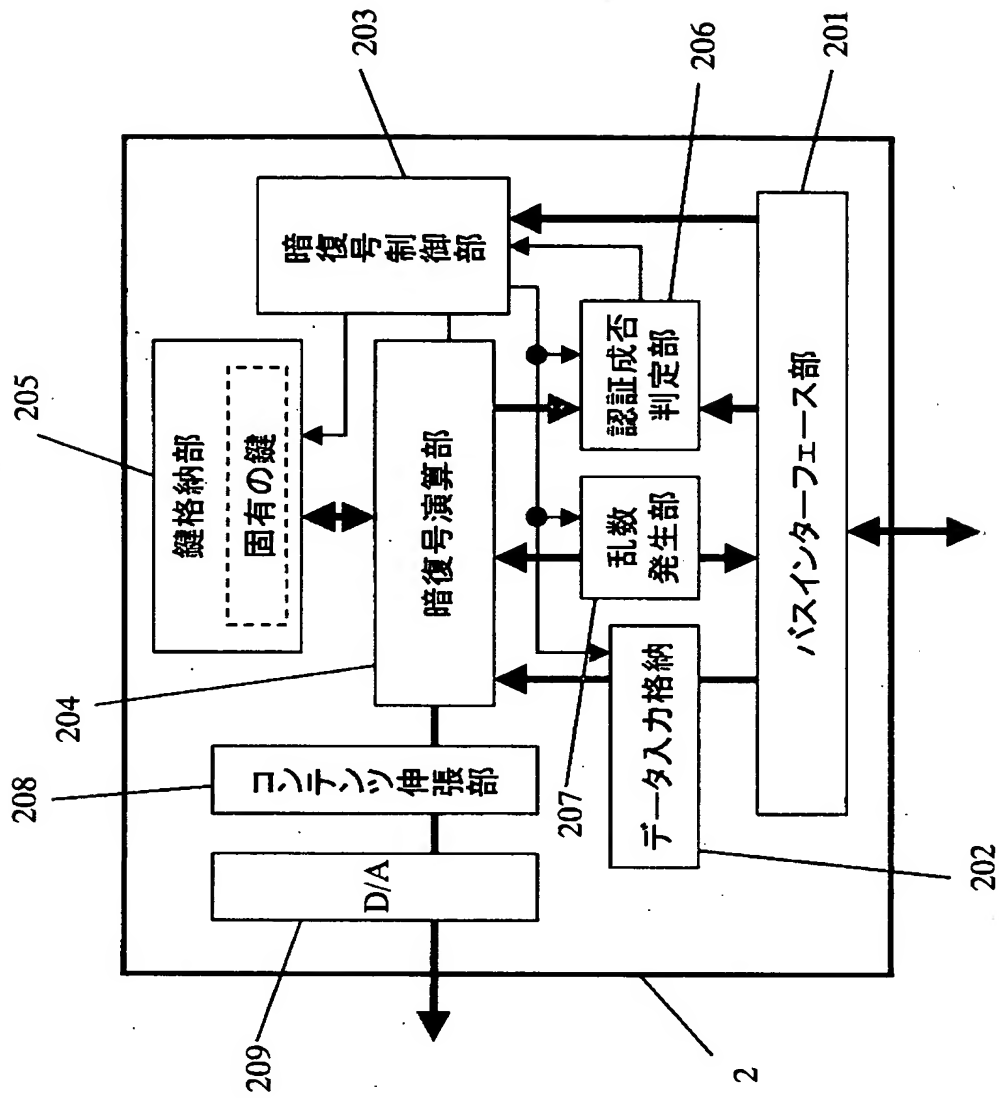
【図9】



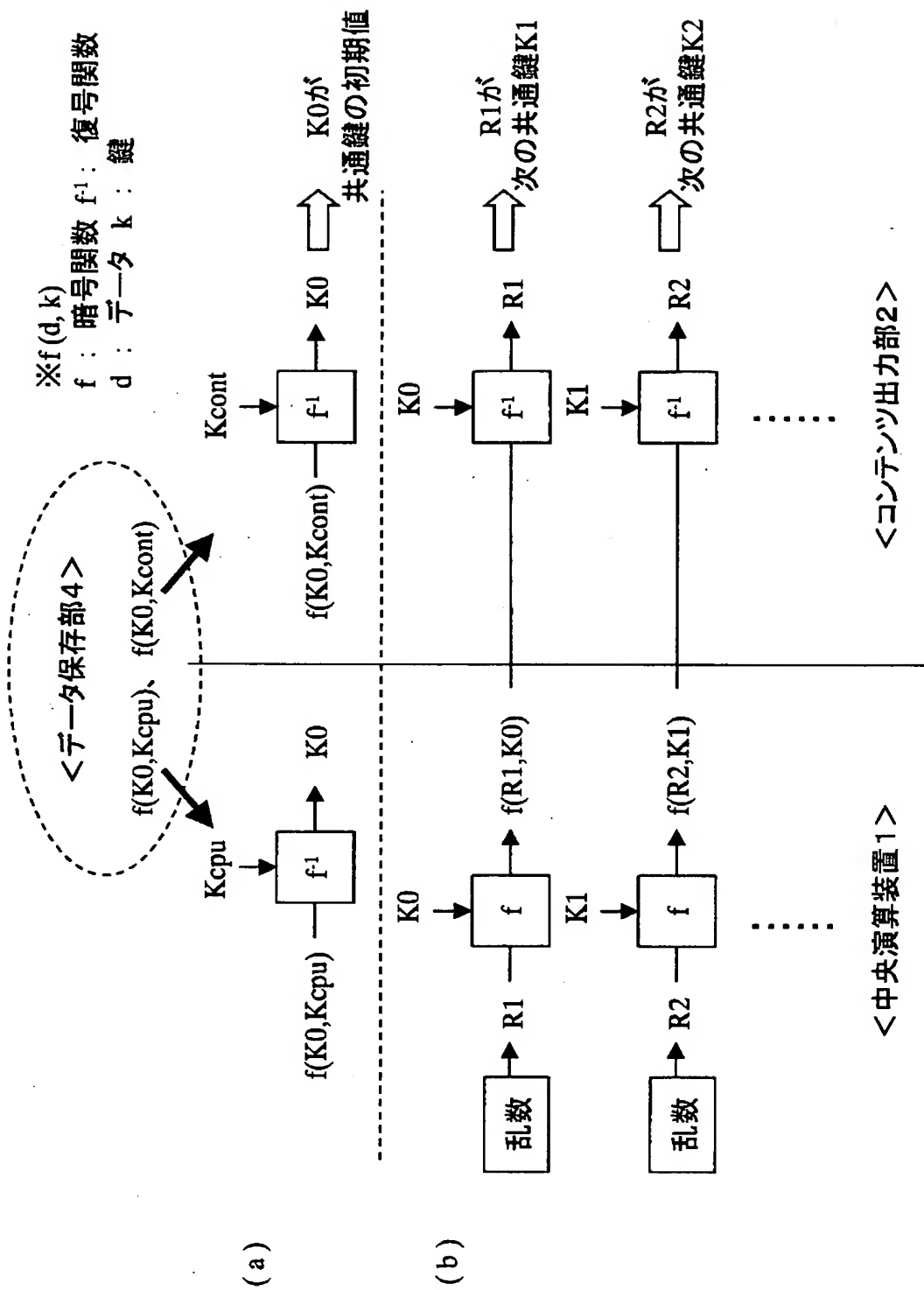
【図10】



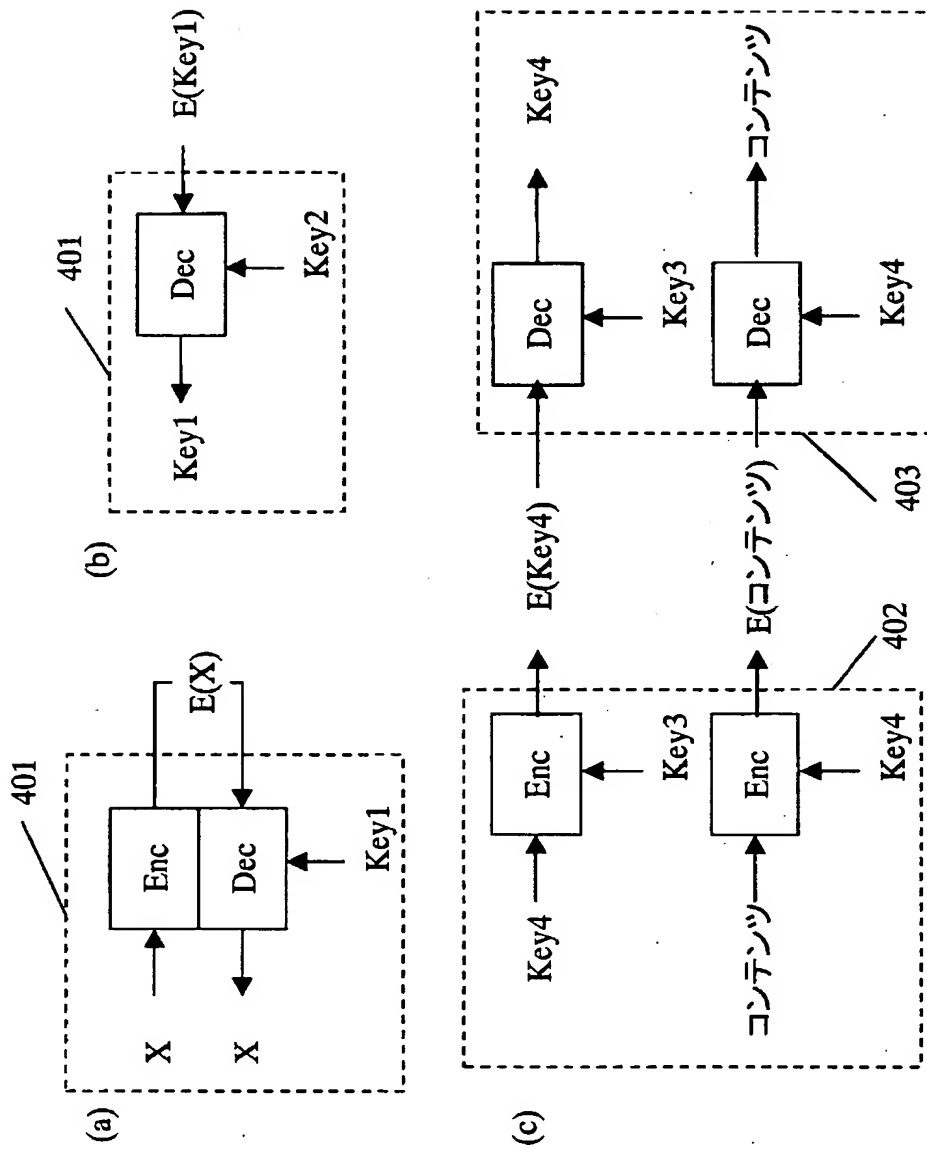
【図 11】



【図12】

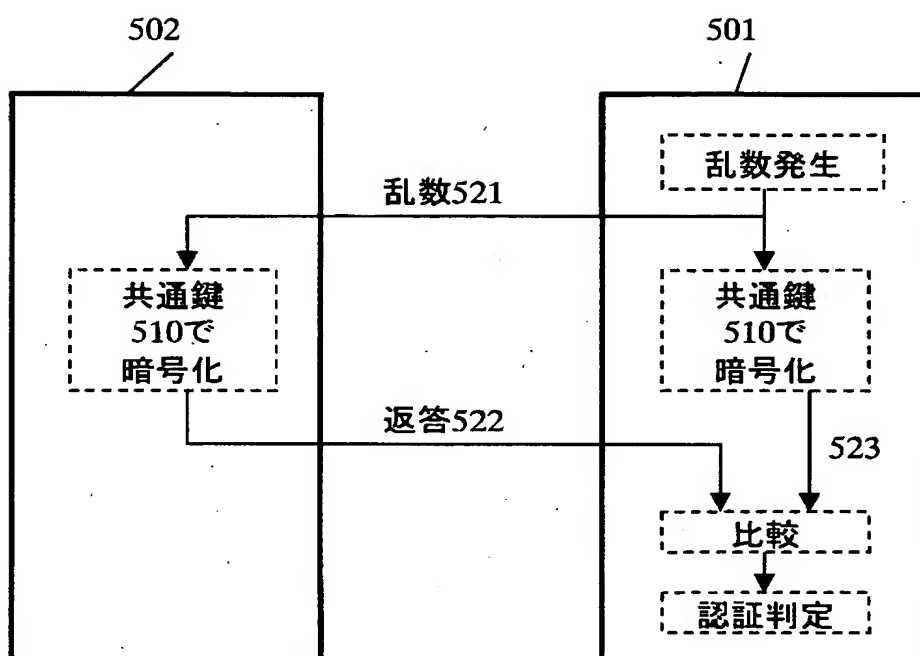


【図13】

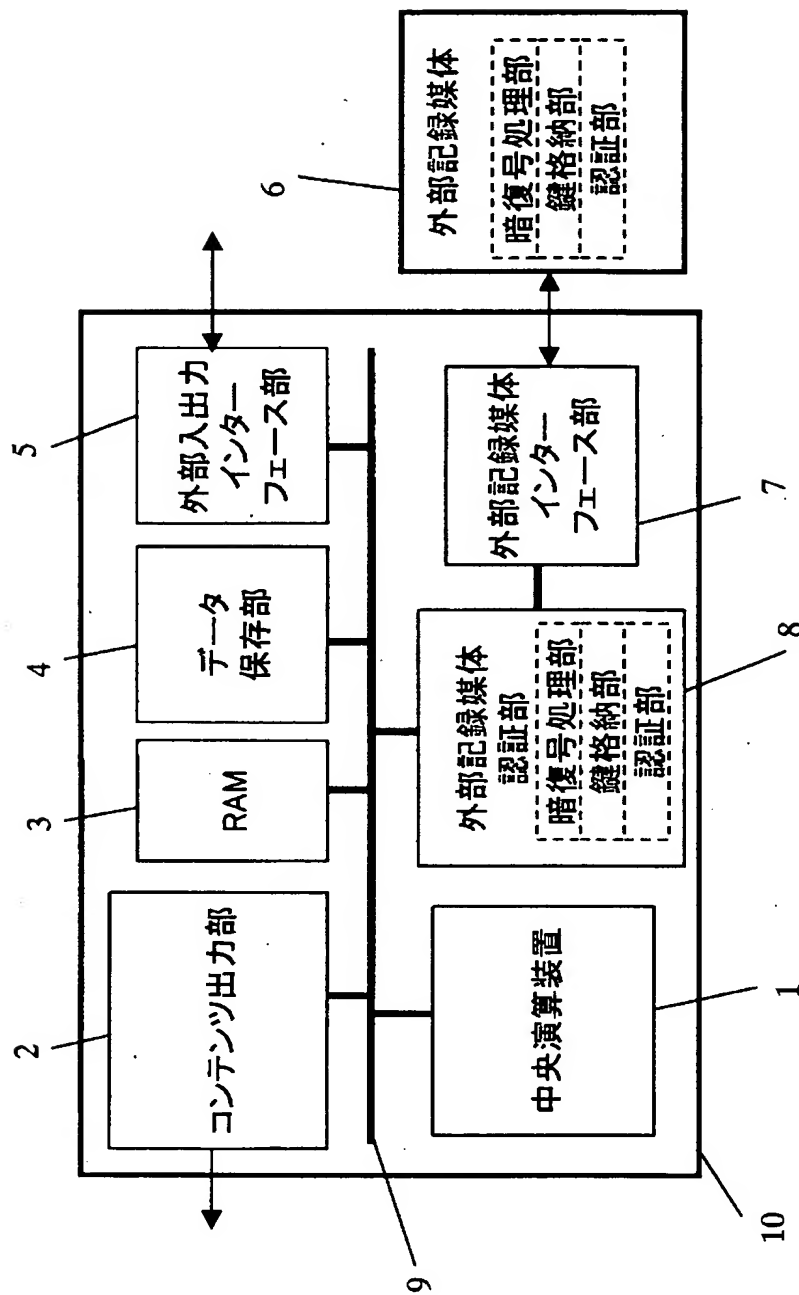


※Enc:暗号演算部 Dec:復号演算部

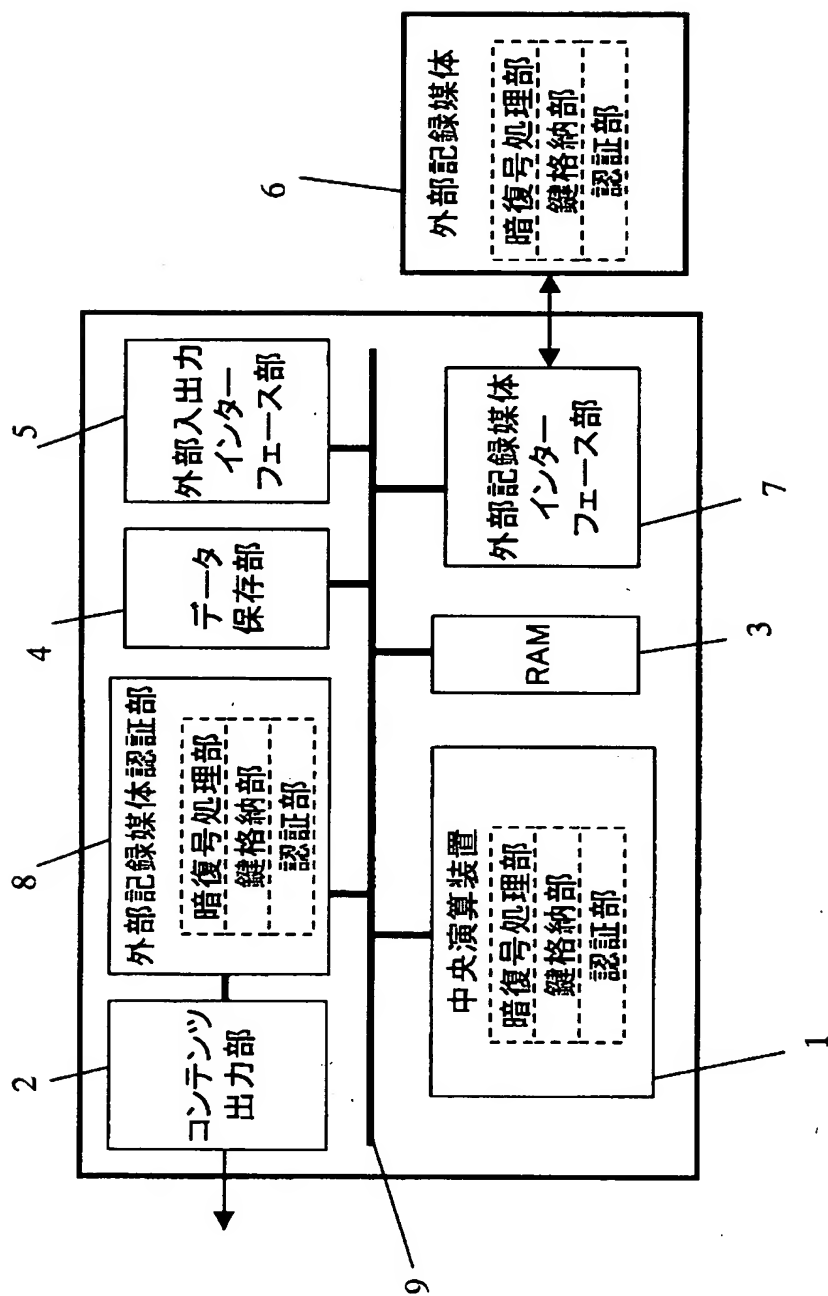
【図 1 4】



【図15】



【図16】



【書類名】 要約書

【要約】

【課題】 従来の、任意の外部プログラムをダウンロードして実行できる装置では、外部プログラムの実行によって、中央演算装置が暗号化されていないコンテンツを複製などの不正な操作を行うことを防ぐことができない。

【解決手段】 中央演算装置に暗復号処理機能と復号データ格納機能と復号データ転送先アドレス監視機能を内蔵させることで、許容されている生のコンテンツの出力先を制限する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社